Banque : les nouvelles menaces agissent après l'identification du client

Les nouveaux virus se jouent du processus d'authentification le plus sévère. En effet, les cyber-criminels modifient leur tactique, pour faire face aux défenses mises en place par les banques. C'est ce qu'a expliqué Alex Shipp, spécialiste antivirus chez Messagelabs, un spécialiste de la gestion de la messagerie électronique, lors de RSAconference, une réunion d'experts en sécurité informatique, qui s'est tenue en Californie du 13 au 17 février.

Voici comment fonctionne le dernier cheval de Troie, rapporte *Zdnet.com*, qui se fait l'écho de la conférence. Il suffit que l'internaute télécharge une anodine carte de v?ux, par exemple, pour hériter d'un exécutable. Ce dernier s'installe dans le navigateur. Le virus attend alors que l'internaute, dûment identifié par sa banque, soit connecté avec elle, pour se déclencher et transférer de l'argent hors du compte. D'après Alex Shipp, ces nouveaux chevaux de Troie représenteraient la troisième menace recensée aujourd'hui. **Virus anti-confiance** En attendant, en Europe, les bonnes vieilles méthodes continuent d'avoir cours. Des pirates non identifiés auraient détourné 200.000 euros entre août 2004 et mars 2005, à l'aide de virus qui ont piraté les codes d'accès aux comptes bancaires d'internautes au poste de travail mal protégé, rapportait *Le Parisien*, le mois dernier. Et en Italie, cette même somme, escroquée sur diverses comptes, transitait vers des comptes bancaires de pays étrangers. Jusqu'à ce que la police ne les bloque, et arrête 70 responsables du phising à l'origine de la fraude, d'après le webzine spécialisé *I-dome.com*. Pis, si les tentatives, comme celle du Crédit Lyonnais, ne font pas nécessairement de victimes parmi les clients, elles n'en risquent pas moins d'éroder sérieusement la confiance dans la banque en ligne.