Phishing : retour à la normale en février

RSA, la division sécurité d'EMC, vient de publier son 13e rapport d'activité mensuel du phishing dans le monde. Et depuis février 2006, date du premier rapport de RSA, les tentatives d'hameçonnage n'ont pas ralenti sur la toile. En février 2006, la filiale du spécialiste du stockage dénombrait 102 marques utilisées pour attirer le chaland trop naïf. En février 2007, ce chiffre s'élève à 153. Même s'il est loin de constituer un record, révélé en décembre 2006 avec 205 marques attaquées, il est significatif de la progression du phénomène.

Malgré tout, après une recrudescence des attaques constatées fin 2006 et en janvier 2007, le mois de février annonce un retour à la "normale", selon la cellule anti fraude de RSA (AFCC) qui s'appuie sur un réseau d'analyse des activités de 150 institutions financières dans le monde pour établir son rapport. La répartition des pays visés ne bouge pas beaucoup. Avec 67 % des attaques, les établissements américains constituent les premières cibles des attaquants (66 % en janvier 2007). Les banques du Royaume Uni arrivent en 2e position (15 % des attaques), suivies de l'Espagne (4 %), du Canada (3 %) *ex-æquo* avec l'Italie. Signalons cependant que la France et la Grèce font leur entrée dans le classement du Top 10 avec 1 % des attaques chacune.

Pas de grand changement non plus du côté des zones d'activité du hameçonnage. Les Etats-Unis restent incontestablement le premiers pays hébergeur des sites de phishing avec 75 % du total des attaques (sans changement par rapport au mois précédent). Avec respectivement 6 % et 4 %, l'Allemagne et la France arrivent en deuxième et troisième position. Le reste se dilue entre le Royaume Uni (3 %) et la Chine, Hong Kong (qui avec le Danemark reviennent dans la liste), le Canada, la Russie et les Pays-Bas avec 2 % chacun.

Fermeture de comptes frauduleux

Pour le reste de l'année, RSA maintient ses prévisions. A savoir que, face à une meilleure protection des établissements financiers, les pirates vont lancer de nouvelles formes d'attaques à partir de chevaux de Troie, chargés d'introduire des spyware dans les systèmes informatiques, et le *pharming* qui consiste à rediriger les internautes vers de faux sites officiels en piratant les serveurs DNS (Domain Name Server) et en changeant les adresses IP.

Mais il n'y a pas que de mauvaises nouvelles. Pour ainsi dire accusé de complicité, le service américain de paiement en ligne e-Gold a fermé nombre de comptes d'utilisateurs frauduleux. Ces derniers se servaient du service pour effectuer leurs transactions douteuses. Les comptes où apparaissaient des échanges financiers avec les fraudeurs ont également été bloqués, selon e-Gold. Il restera à vérifier que la mesure porte ses fruits. Mais il est à craindre que les fraudeurs se tourneront vers d'autres solutions de paiement en ligne, aux Etats-Unis comme à l'étranger.