

# Phishing d'avril : moins de banques visées selon RSA

L'internaute croque moins souvent dans l'asticot. C'est du moins ce que met en exergue la 3ème édition du « Phishing Intelligence Report » publiée par RSA, regroupant les informations recueillies par sa Cellule Anti-Fraude (AFCC) qui surveille le réseau 24h sur 24.

Sa mission est de détecter les attaques par phishing ou hameçonnage, mais aussi par pharming, une opération qui consiste à installer un site factice contenant des copies de pages d'un site officiel dans le but de recueillir des informations confidentielles sur les utilisateurs. En piratant les serveurs DNS (Domain Name Server) et en changeant les adresses IP, les utilisateurs sont dirigés automatiquement sur des sites fictifs. Le rapport de RSA Cyota présente des statistiques sur les attaques identifiées via son réseau d'analyse mondial. Ces rapports analysent les tendances recueillies par les experts de cette cellule. La progression des attaques de phishing ciblant les banques hors des États-Unis se poursuit. 57% des banques touchées sont situées hors du territoire américain, notamment en Espagne et en Italie. Cependant même si le nombre de banques (hors États-Unis) ciblées par ces attaques continue de progresser, le volume des attaques ciblant des banques aux États-Unis reste toujours plus élevé. Selon les statistiques observées en avril 2006, les US figurent à la première place des pays qui hébergent des sites d'où sont lancées des attaques de phishing. Deux tiers des attaques de phishing proviennent ainsi de sites web hébergés aux États-Unis. La France est classée en 6ème position. Il y a eu une baisse significative du nombre de groupes bancaires ciblés par des attaques de phishing en avril. Après un « plus haut » en mars avec 127 groupes ciblés en mars 2006, le nombre d'institutions ciblées a baissé de 25% à 93. Les résultats de mai 2006 permettront de savoir s'il s'agit d'une tendance lourde. A noter que la tendance actuelle du côté des hackers est le phishing ciblé. Ce dernier repose sur un principe simple, le garnement de la toile procède dans un premier temps au vol d'identité pour en connaître davantage sur sa cible puis il réalise une attaque bien ficelée, beaucoup plus efficace et dangereuse. Ce rapport du RSA est donc peut-être l'arbre qui cache la forêt et il va falloir attendre un peu pour voir si cette tendance se confirme.