E. Tonnelier, Pandasoftware: Lorsque vous braquez une banque, est-ce que vous alertez la presse?

Comment évolue le phishing ? Dans le monde anglo-saxon, le phishing existe déjà depuis deux ans. Mais, autant à l'origine c'était une pratique qui visait à déranger, autant maintenant ses visées sont devenues purement frauduleuses. Depuis 2005, les attaques se sont multipliées contre les banques en France, avec la plus récente du Crédit Lyonnais, ou avant du Crédit Mutuel. Celle contre le Crédit Lyonnais montre que les techniques deviennent plus sophistiquées, puisque l'attaque s'est déroulée en deux vagues, la deuxième qui se fait passer pour un correctif. Jusqu'à présent, les techniques de phishing sont restées de qualité médiocre. Par exemple, l'URL vers laquel est dirigé l'internaute n'est pas très proche de celle de la banque. Comment se prémunir contre le phishing ? Depuis quelques mois, nous avons intégré les caractéristiques du phishing dans notre base de donnée virale, en prenant en compte, par exemple, la liste des établissements réputés pour être victimes de ces attaques, ou encore des objets comme une demande de password. Et, dans notre lettre d'alerte aux clients, nous mentionnons également ces attaques. Heureusement, de plus en plus d' internautes s'équipent d'antivirus. Du coté des banques, cela devient une préoccupation prioritaire. Même si peu de personnes tombent dans le panneau, il suffit du fait que l'on parle de ce problème au journal de 20 heures pour que la confiance soit entamée. Et pour une banque, c'est vital. Comment évolue le risque aujourd'hui ? Il y a deux ans, on parlait tout le temps des nouveaux virus. Maintenant, c'est le silence radio. A mon avis, cela dénote le fait que les nouveaux pirates n'ont pas intérêt à attirer l'attention sur eux. Quand vous braquez une banque, vous n'appelez pas la presse ! Au contraire, il y a, d'après moi, des man?uvres de diversion. Les éditeurs de logiciels se sont félicités du fait que le ver Kamasutra, qui devait faire beaucoup de dégâts, n'ait finalement rien détruit. Pendant ce temps, deux versions de Baggle, un virus cheval de Troie, se diffusent, sans que personne n'en disent rien?. A suivre? Il existe également un autre type d'attaque très dangereux, dont peuvent être victimes les banques ou les sites de commerce électronique : il s'agit d'attaquer des serveurs DNS, qui redirigent les adresses. Résultat, lorsque l'internaute pense se diriger vers le site de sa banque, il est redirigé vers un autre site qui lui ressemble comme deux gouttes d'eau.