Le phishing, nouveau? En réalité, il date…

Le ‘

phishing‘, que l’on appelle aujourd’hui ‘*hameçonnage*‘, est apparu en 1996. A l’époque, il avait pour objectif d’obtenir des données d’authentification pour entrer sans payer sur le réseau AOL et obtenir des quotas plus élevés de téléchargement.

Le terme n’est apparu pour la première fois qu’en 1997, dans un magazine d’informatique grand public. Mais comme le confirme Gunter Olmann, directeur de la X-Force d’Internet Security Systems, « *Les choses ont bien changé depuis?* » Au cours de cette décennie, les pirates se sont adonnés au phishing en utilisant des moteurs de spam (émission en masse de courriels indésirables), des canaux IRC ou IM, des bandeaux publicitaires web et même des bulletins d’information pour attirer leurs victimes potentielles vers des sites web factices ou malicieux. Du ‘simple’ vol de mots de passe et d’identifiant par quelques individus, on est passé à une activité criminelle internationale hautement organisée, utilisant des outils spécialisés pour effectuer du blanchiment d’argent, des transferts bancaires internationaux, la fabrication de cartes de crédit et pour usurper l’identité des internautes. En 2001, alors que les entreprises étaient submergées de courriels, les pirates sont parvenus à outrepasser les filtres antispam et, en utilisant des URL glissées dans des textes HTML inclus dans des courriels, à tromper les destinataires en les incitant à visiter des sites web factices qui collectent, à leur insu, des informations confidentielles telles que leurs données bancaires. Les courriels de phishing sont ensuite devenus de plus en plus sophistiqués, paraissant toujours ‘plus vrais’. Pour Gunter Olmann, « *on évalue aujourd’hui à 5% la proportion des destinataires qui est mystifiée, soit une personne sur 20?* » Même s’ils ne font la une des médias que depuis peu, les pirates du phishing ont considérablement affûté leurs moyens d’attaque. Par exemple, ils sont aujourd’hui capables de s’attaquer aux serveurs de noms Internet (DNS, *Domain Name Server*) qui font correspondre les noms des sites Web à l’adresse IP réelle des serveurs. Ainsi, lorsqu’il entre dans son navigateur l’adresse URL du site Internet qu’il veut visiter, l’internaute n’a aucun moyen de détecter que sa requête a été redirigée vers un site pirate. Ils pratiquent aussi le phishing ciblé (*spear phishing*), en installant des codes espions (*keyloggers* ou chevaux de Troie) sur un groupe limité de PC cibles et/ou en utilisant des listes de diffusion restreinte, ce qui rend quasi impossible la protection par un système classique à base de signature. « *Dans un avenir proche, ces attaques ne peuvent que continuer à évoluer*« . Compte tenu des tactiques adoptées précédemment, il est probable que les pirates vont tirer avantage de la généralisation de la voix sur IP – dans un contexte tant professionnel que privé – et profiter de l’anonymat que procure cette technologie pour amener les utilisateurs à fournir des détails sur leurs données d’identité et d’authentification. « *Il sera intéressant de voir l’évolution de ce phénomène en ‘ph’ (phishing, pharming, ?) et quel nom sera attribué à ses nouvelles attaques : ‘*Phiting*‘ pour phishing via la téléphonie sur IP ou ‘*Phreaking*‘ ?*«