Le nombre de menaces a explosé, le Web nouveau vecteur d'attaques

Comme ses concurrents éditeurs de sécurité, Sophos fait un constat simple. 2007 illustre un profond changement dans les vecteurs d'attaques utilisés par les pirates. Si jusqu'à présent le courriel était leur outil préféré, aujourd'hui le Web est devenu le moyen le plus utilisé pour piéger les internautes.

Les pirates exploitent à coeur joie les failles des pages URL, qu'il s'agisse d'image, de spoofing d'adresse, d'URL piégé… Ils utilisent également les possibilités des sites communautaires (type YouTube) et Web 2.0 qui permettent de placer encore plus de malwares, notamment dans les photos et les vidéos. Il faut dire aussi que les utilisateurs savent de mieux en mieux se protéger contre les virus diffusés via les messageries électroniques.

Ainsi, au cours du premier trimestre 2007, Sophos a identifié 22.864 nouvelles menaces, soit plus de deux fois le nombre découvert pendant la même période de 2006 (9.450). Dans le même temps, le pourcentage de courriels infectés est tombé de 1,3% au premier trimestre 2006, soit un message sur 77, à 0,4% seulement (1 message sur 256) en 2007.

Dans le même temps, l'éditeur a identifié une moyenne **5.000** nouvelles pages Web infectées par jour, principalement par des chevaux de Troie.

Sophos précise que la majorité des pages infectées, soit 70%, sont des sites authentiques rendus vulnérables aux attaques car ils ne disposent pas des correctifs de sécurité, ont été mal programmés ou ne sont pas entretenus par leurs propriétaires.

Parmi les autres sites identifiés, 12,8% hébergent des scripts malveillants et 10,7% sont infectés par des programmes malveillants Windows. Des adwares ont été découvert dans 4,8% des pages, et des ?diallers' pornographiques (des programmes redirigeant automatiquement l'utilisateur vers une adresse surtaxée) sur 1,1% d'entre elles.

« Le plus inquiétant dans ces affaires est que de nombreux sites Web deviennent les victimes des pirates parce que leurs propriétaires ne les tiennent pas à jour, et en particulier n'appliquent pas les correctifs de sécurité adéquats », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud. *« Les utilisateurs d'Internet supposent que des sites tels que la page d'accueil des Miami Dolphins sont parfaitement sûrs, mais en ciblant un vaste palette de pages Web, les pirates parviennent à infecter un plus grand nombre d'internautes. N'importe quel site insuffisamment maintenu peut un jour ou l'autre être victime de ces agissements. »*

Rappelons que selon le groupe WhiteHat Security, huit des dix plus grands sites du 3W sont vulnérables, permettant à des hackers de récupérer des données confidentielles.

Il faut noter que la France est le 7e pays de la planète à héberger des sites piégés, loin derrière la Chine (1er) et les Etats-Unis.