Record d'attaques via le Web au premier semestre 2007

Les menaces diffusées via le Web ont connu une explosion au cours du premier semestre 2007. C'est l'une des conclusions de l'étude de l'éditeur britannique Sophos, étude portant sur le cybercrime dans le monde.

Le réseau mondial de stations de surveillance de Sophos a identifié, rien qu'au cours du seul mois de juin, une moyenne de 29.700 pages Web infectées par jour, alors que ce nombre n'était que de 5.000 au début de l'année.

En se basant sur un échantillon d'un million de ces pages, les experts de Sophos ont déterminé que 28,8 % d'entre elles hébergent des *malwares* et que 28,0 % sont bloquées à cause de de contenu pornographique ou de jeux d'argent. 19,4 % sont des pages créées par des spammeurs et 4,3 % sont classées comme sites illégaux, lorsqu'elles sont par exemple identifiées comme sites de phishing ou de vente de logiciels piratés.

Parmi les sites contenant du code malveillant, un sur cinq seulement a été conçu spécifiquement dans ce but, tous les autres étant des pages légitimes infectées par les pirates.

« Le Web est désormais le vecteur d'attaque préféré des cybercriminels animés par des motivations financières?

Le recours à cette stratégie, même si elle les a éclipsés, n'a en revanche pas mis fin à la diffusion des menaces par les courriels, dont le nombre moyen ? 1 courrier électronique affecté sur 337, soit 0,29 % de l'ensemble des messages échangés ? reste étrangement stable.

A ce titre, l'utilisation de fichiers joints à des messages de spam revient en force. Afin d'éviter la détection par les solutions de filtrage les moins performantes, les spammeurs utilisent désormais fréquemment des fichiers PDF contenant une version graphique de leurs messages commerciaux, dans l'espoir d'attirer de nouveaux clients.

Dernier constat de l'étude, le premier semestre 2007 a connu une résurgence de la diffusion de logiciels malveillants via les périphériques de lecture-écriture externes. Il ne s'agit cependant plus des disquettes du début des années 1990, mais des clés USB.

Sophos met en cause l'exploitation par les pirates de la **fonction 'auto-run**' que certains utilisateurs activent sur leur PC sous Windows pour faire s'exécuter automatiquement un programme dès que la clé est insérée. Le ver LiarVB-A, qui diffuse des informations sur le Sida et le VIH via les clés USB, est un bon exemple.

Le Rapport sur la Sécurité de Sophos peut être téléchargé sur www.sophos.com.

Apache ou Microsoft, personne n'y échappe? L'intérêt du Web pour les cybercriminels est de pouvoir rapidement et facilement contaminer un grand nombre de pages Web à partir d'un unique fichier infecté partagé par de multiples sites, sans rapport les uns avec les autres mais tous hébergés par le même serveur Web.A ce titre, ce sont d'abord (51 %) les serveurs Apache qui sont affectés par ces attaques, suivis de près par les serveurs Microsoft IIS (43 %). Une nouvelle démonstration que le problème est loin de n'affecter que les plates-formes Microsoft !