Piratage: les pages 'légitimes' restent la cible privilégiée des attaques

Les statistiques établies durant le mois de juillet 2007 par Sophos et son réseau mondial de surveillance et d'analyse des menaces révèlent une hausse significative de la famille de menaces Web **Mal/ObfJS**: son taux est passé, en un mois, de 1,8% à 17,3%. Le rapport mensuel confirme l'augmentation des menaces déjà évoquée dans le rapport semestriel de l'éditeur.

Mal/Iframe conserve la pole position du classement, avec plus de la moitié du total des menaces issues du Web.

Les experts des Sophos Labs notent que la domination de ces deux menaces met en évidence la technique de **téléchargement « à la volée »** pratiquée de plus en plus par les cybercriminels, ainsi que l'usage de plus en plus fréquent de **code Javascript camouflé** au sein de sites Web infectés.

« Le danger que le Web représente pour la sécurité n'est toujours pas pleinement pris en compte par de nombreuses entreprises, ce qui offre de vastes possibilités à des pirates avides d'informations confidentielles », commente Michel Lanaspèze, directeur Marketing et Communication de Sophos France / Europe du Sud.

« Il n'est pas surprenant que des pages Web légitimes soient la cible de ces attaques : les entreprises n'interdisent en général pas à leurs employés d'y accéder, et le trafic quotidien de visiteurs évite au pirates de trouver de nouvelles astuces pour piéger leurs victimes. »

La Chine demeure le principal pays hébergeant ces pages Web infectées par du code malveillant. Le nombre de pages hébergées par la Russie connaît également une augmentation importante par rapport au moins de juin, où sa part ne représentait que 3,5%. Cette croissance s'explique par le grand nombre de pages russes infectées par Mal/Iframe et par Mal/ObfJS ces dernières semaines.

« Il est important que les pays comprennent que les pirates n'ont pas de préférence quant au lieu géographique de leurs attaques. Ils visent tout hébergeur Web vulnérable qu'ils parviennent à identifier, ce qui signifie qu'aucun pays n'est à l'abri. Pour les entreprises, le seul moyen de se protéger est de mettre en place des solutions sécurité de dernière génération et de s'assurer que les utilisateurs ne mettent pas leur réseau en danger par un comportement irresponsable. »