Les ‘malwares’ sont liés au cyber-crime

Le

cheval de Troie (*Tojan*), ce programme malicieux qui s’installe sur le poste informatique à l’insu de son utilisateur et attend son heure pour dérober des informations déclencher une attaque, est devenu en quelques années l’arme principale des mafieux en ligne.

Ce n’est donc pas une surprise si les Panalabs, les laboratoires d’observation des menaces contre nos outils informatiques, ont constaté au deuxième trimestre 2006 que plus de la moitié (54,4 %) des ‘*malwares*‘ détectés appartiennent au genre cheval de Troie. Ils étaient moins de la moitié (47 %) au trimestre précédent !

Car les auteurs de ces programmes malicieux cherchent désormais à tirer profit de leur production en les transformant en outils de racket et dérives mafieuses afin d’en obtenir des retours financiers.

Ce type de code malicieux est très flexible, ils peuvent être utilisés pour mener toute une série d’actions sur les ordinateurs infectés : vol d’informations confidentielles (données bancaires notamment), téléchargement de programmes malveillants, etc.

Autre menace qui ne cesse de grossir, et que l’on constate au quotidien par la multiplication des e-mails spammés sur nos messageries, les **bots**. Autre type de programme malveillant, ils sont utilisés pour créer des réseaux de PC zombies, des serveurs de spam, vendus ou loués au plus offrant. Ils occupent la deuxième place des nouveaux malwares détectés (16%), et enregistrent une augmentation de quatre points par rapport au trimestre précédent.

Suivent les ‘**backdoors**‘, des trous béants qui n’attendent qu’à être exploités pour permettre aux pirates de pénétrer un système, qui ont compté pour 12,1% des nouveaux malwares. Puis les numéroteurs pour seulement 3,8%. Enfin, les adwares et les spywares ont représenté 1,7% de l’ensemble.

Comme l’indique Luis Corrons, le directeur de PandaLabs, « *ces chiffres indiquent que les pirates concentrent leurs efforts sur des activités lucratives, en concevant un nombre croissant de chevaux de Troie et de bots. Le plus grand danger réside dans le fait que ces malwares sont très discrets. Ils s’installent et agissent subrepticement, sans que les utilisateurs ne remarquent les symptômes habituels d’une infection. Par conséquent, les victimes ne savent pas que leur ordinateur est utilisé pour dérober leurs informations ou celles de tiers. Ce faux sentiment de sécurité agit en faveur des pirates*. »