

# Menaces sur les IT : les attaques viennent des US

Les chercheurs du 'lab' Symantec de Cupertino ont fait le constat qu'au deuxième semestre 2006, le tiers des attaques de systèmes informatiques dans le monde provenaient des Etats-Unis, qui demeurent la terre la plus fertile pour toutes les menaces qui pèsent sur nous, via le spam, le phishing et les codes malveillants.

La Chine, de plus en plus pointée du doigt par les autorités américaines comme étant la source de tous les maux qui menacent l'informatique, ne pointe en réalité qu'en seconde place avec 10 % des attaques, suivie par l'Allemagne avec 7 %.

Les Etats-Unis détiennent également, toujours selon Symantec, le triste record des réseaux de 'bots' (zombies). Rappelons qu'un 'bot' est un ordinateur compromis qui est contrôlé à distance par un pirate et inséré dans un réseau de 'bots' exploité comme pompe à spam ou pour d'autres opérations toutes aussi illégales.

Ces réseaux s'appuient sur des serveurs mafieux, ils seraient 4700 selon Symantec, en recul de -25 %, qui alimentent un réseau de 'bots' estimé à 6 millions d'ordinateurs dans le monde, en recul de -25 %. On notera cependant que 26 % des 'bots' seraient en Chine?

En revanche, dans le même temps, le trafic du spam aurait progressé de 5 %, en particulier avec la multiplication des offres financières et d'opérations boursières, jusqu'à atteindre 59 % du trafic total des messageries.

Plus dangereux, Symantec affirme que les Etats-Unis hébergeraient plus de la moitié des '*serveurs d'une économie souterraine*' créée pour organiser des réseaux de transactions clandestines basées sur des données volées.

Un tel réseau permettrait d'exploiter des données confidentielles comme un numéro de carte bancaire ou de sécurité sociale dans les deux heures à deux semaines qui suivent le vol?

Pire encore, ce réseau serait à l'origine d'un commerce mafieux des informations dérobées. Et Symantec de citer des prix, de 1 dollar pour un numéro de carte bancaire à 14 dollars pour une identité complète, nom, date de naissance, sécurité sociale, compte bancaire et carte bancaire !

Dernières remarques, 77 % des attaques ciblent en priorité le navigateur Internet Explorer de Microsoft. Et Symantec anticipe l'émergence d'attaques contre le système d'exploitation Windows Vista. Ainsi que de campagnes de phishing visant les joueurs en ligne et consistant à usurper l'identité des sites de jeux massivement multi-joueurs.