Salon Infosecurity 2007 : va-t-on vers le pire en matière de logiciels malveillants ?

Le premier ver (« *worm* ») a déjà 25 ans. Il est né (chez Xerox) de l'idée d'utiliser la puissance des ordinateurs dormants (donc la nuit et le week-end, principalement) afin de réaliser des calculs longs, qui étaient alors exécutés de façon répartie par les différents ordinateurs du réseau. Les premiers virus sont apparus à peu près au même moment. Ils fonctionnaient sur le même principe mais avaient des objectifs malveillants. Ils étaient plutôt motivés par des défis techniques.

Selon les résultats de l'étude, l'évolution la plus importante de cette industrie du logiciel malicieux concerne le passage « du défi au profit », avec des variations au fil des années : le vol d'informations et la vente d'accès par envoi de *spam* sont devenus les deux principales motivations des programmeurs de *malware*. L'étude met également en évidence la saisonnalité des attaques, cette saisonnalité étant basée sur l'ingénierie sociale : alors que l'utilisation des « pseudo cartes postales » culmine sur les 2 mois de juillet et août, par des campagnes s'étalant sur 1 mois ou deux, l'utilisation des tests gratuits de version béta de programmes ludiques correspond souvent à une opération ponctuelle d'une journée.

On constate également une évolution dans le déclenchement des attaques : l'activation des programmes malveillants (restés dormants jusque-là dans les ordinateurs infectés) n'est plus commandée par un serveur central, mais par un réseau décentralisé de serveurs… bien sûr plus difficile à détecter.

A partir de cette étude, et en termes de projections pour l'avenir, les experts d'ESET nous annoncent que :

– les créateurs de logiciel peuvent faire pire (car ils se sont professionnalisés, et aussi parce que les profits en jeu sont plus importants, d'où une capacité d'investissement en R&D plus conséquente pour trouver de nouvelles failles)

– les attaques seront plus ciblées et personnalisées

– l'architecture logicielle des programmes d'attaque deviendra encore plus modulaire qu'aujourd'hui, par la réutilisation de codes existants et par l'augmentation de composants « faits maison ».

Pas très rassurant, tout cela… Heureusement, l'étude d'ESET révèle par ailleurs que les techniques de défense s'améliorent nettement (meilleur filtrage des emails, évolution vers plus d'heuristique et vers des capacités de désinfection plus efficaces). Et surtout, grâce au développement des politiques de sécurité en entreprise (en particulier les actions de sensibilisation), la connaissance des menaces s'améliore et se propage parmi les utilisateurs.

Reste que, si l'efficacité des boucliers s'améliore, ESET n'en conclut pas moins que l' « on aura toujours besoin de se défendre »…