Des logiciels de piratage vendus clés en main sur le Net

- Informatique - Internet -

Date de mise en ligne : vendredi 25 mai 2007

C'est un nouveau business pour les développeurs peu scrupuleux. Les outils de piratage sophistiqués sont désormais vendus en ligne comme des produits classiques, avec support et mise à jour inclus.

Votre PC est peut-être un cyber-soldat sans que vous le sachiez. Le 27 avril dernier, une bataille électronique d'envergure opposait des pirates russes et estoniens. Au final, les Russes ont pris le dessus en bloquant plusieurs dizaines de pages Web sur des sites importants, notamment celui de la principale banque estonienne, l'Eesti Uhispank. Plus d'un million de PC à travers le monde auraient été impliqués dans cette affaire, sans que leur propriétaire n'en sache rien.

Pour mener leur attaque, les pirates ont en effet souvent recours à des machines zombies : des ordinateurs d'utilisateurs lambda dont ils ont discrètement pris le contrôle à distance. Ces réseaux de PC constituent des botnets. La technique n'est pas nouvelle, mais elle prend une nouvelle ampleur avec l'arrivée de logiciels d'administration de botnets toujours plus simples d'emploi. Des outils qui peuvent transformer n'importe quel internaute en pirate informatique.

Spam, piratage, diffusion de contrefaçons...

L'un de ces logiciels a été repéré la semaine dernière par l'éditeur d'antivirus Panda Software. Ce programme, connu sous le nom de Mpack, est utilisé pour télécharger des malwares sur des ordinateurs distants en exploitant plusieurs vulnérabilités. Une fois installés, ces malwares permettent à un pirate de se livrer à toutes les activités de son choix, en particulier illégales : envoi de spams, blocage de serveurs, diffusion de contrefaçons ou d'images pédophiles...

D'après le laboratoire de recherche de Panda Software, MPack a déjà été utilisé à plusieurs reprises. Un couteau suisse pirate « qui a servi à infecter 160 000 ordinateurs ». Dans le même genre, Zunker a été utilisé pour gérer un réseau de plusieurs milliers d'ordinateurs zombies et cela à partir de 54 pays. Mpack et Zunker ne sont pas seuls. Des dizaines d'autres programmes existent sous des noms tout aussi explicites : Robot GT, Agobot Dsnx ou encore Sdbot. Sans parler de la constellation de générateurs de virus et autres chevaux de Troie, comme le célèbre VBS Worms generator d'un pirate nommé [K]Alamar.

Des outils pirates vendus avec un an de support

Derrière tout cet attirail électronique se cache aussi un juteux marché parallèle. Panda Software explique que le logiciel MPack est vendu sur certains forums Internet à 700 $ environ (environ 500 euros). Les créateurs offrent un an de support gratuit avec chaque version de leur outil. « MPack offre les mêmes types de services que des programmes licites, par exemple, des mises à jour. Les mises à jour de MPack sont de nouvelles versions de l'application comprenant de nouveaux exploits [techniques de piratage, NDLR] pour profiter des dernières vulnérabilités découvertes. Une nouvelle mise à jour est disponible tous les mois en moyenne et coûte entre 50 et 150 $ [soit 35 à 110 euros, NDLR] », explique dans un communiqué Luis Corrons, le directeur technique de PandaLabs.

Et se protéger de ces outils pirates ne semble pas une mince affaire. Dans le cas d'un site Internet comme d'un ordinateur, le meilleur moyen consiste, comme toujours, à s'assurer de disposer en permanence des dernières mises à jour de sécurité, notamment celles de Microsoft. Evidemment, pare-feux et antivirus sont aussi conseillés.

Post-scriptum :

http://www.01net.com/article/349733.html