Les nouveaux pirates du web cherchent le profit, et non plus la gloire

Technologie

Posté par: Visiteur

Publié le : 23-11-2007 22:18:01

Finis les défis de jeunes "hackers" pour la gloire, place aux cyber-criminels organisés qui agissent dans l'ombre à des fins lucratives: les nouvelles attaques informatiques sont de plus en plus sophistiquées, selon des professionnels réunis à Paris.

Chaque jour, plus de 200 nouveaux codes malicieux apparaissent, selon Eugène Kaspersky, de la société russe d'anti-virus Kaspersky Lab, de passage dans la capitale pour le salon de la sécurité informatique.

Pour lui, la raison de cette multiplication des attaques est simple: "C'est un business profitable, simple à mettre en oeuvre, à faible risque et aux opportunités croissantes, puisque de plus en plus d'argent circule sur internet".

Les cyber-délinquants sont devenus de vrais professionnels qui rivalisent d'imagination pour dérober des données bancaires ou menacer d'extorsion de fonds des sociétés.

La société F-Secure a par exemple fait état jeudi d'une nouvelle technique permettant de récupérer mots de passe et identifiant au moment même où l'internaute les tape sur la vraie page web de son site bancaire.

Egalement en vogue, les attaques dites de "déni de service" consistent à provoquer l'interruption de service d'un site web, en envoyant des centaines de milliers de requêtes simultanément par le biais d'ordinateurs "zombies" (ou "botnets"), contrôlés à l'insu de leurs utilisateurs. Avec, à la clé, une demande de rançon... souvent acquittée par les sites victimes pour limiter les dégâts.

Autre nouveauté, les programmeurs vendent désormais leur savoir-faire. "Botnets", programmes malveillants de type "chevaux de Troie", failles de sécurité, kits de piratage: tous ces outils "sont mis aux enchères sur des forums, alors qu'auparavant les hackers auraient transmis les vulnérabilités détectées à l'éditeur, en général Microsoft, en échange d'une reconnaissance quelconque comme un stage", explique Mahmoud Denfer, ingénieur chez Trend Micro, développeur d'antivirus japonais.

Dernier critère, la discrétion. Les auteurs d'attaques veillent à ne pas laisser de traces en ayant recours à des intermédiaires, notamment des mules pour transférer l'argent. Les moins chevronnés se contentent de vendre les données confidentielles collectées sur le web.

"Les premiers virus avaient pour but la gloire, le +fun+, et se manifestaient sous une forme très bruyante. Aujourd'hui, l'objectif est devenu vénal et l'utilisateur ne se rend pas compte qu'il est infecté", résume Guillaume Lovet, expert de la société Fortinet.

Conséquence, les enquêtes aboutissent rarement et les arrestations sont rares.

"Le vrai problème, c'est que tout le monde n'a pas conscience" d'avoir été victime d'attaques informatiques ou bien "les victimes ne s'en rendent compte que 6 à 12 mois après", souligne le commissaire divisionnaire Christian Aghroum, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLTIC).

En outre, l'aspect international de cette criminalité rend la lutte "compliquée", poursuit-il: "Toute la planète peut être victime en deux clics de souris du même auteur. Pour remonter le réseau, il faut contourner les barrières des législations étrangères, les problèmes de traduction...".

Face aux ruses des hackers, M. Aghroum recommande à chacun de "se méfier et de ne pas être crédule". Même message du côté des spécialistes de sécurité informatique: ne jamais ouvrir de message non sollicité, ne pas cliquer sur un lien vers son site bancaire et mettre à jour ses outils de protection.

AFP