Sécurité: TrendMicro affiche son pessimisme

Fidèles à leur tradition, les éditeurs de sécurité jouent la carte de l'alarmisme dans leurs visions de l'année 2006. C'est de bonne guerre. Trend Micro ne déroge pas à la règle en dressant un tableau inquiétant des menaces et autres attaques virales ou non qui s'apprêtent à déferler sur nos machines.

Pour autant, s'il faut savoir prendre du recul par rapport à ces discours marketing bien rôdés, il faut bien reconnaître que la tendance dans la sécurité informatique n'est pas à l'amélioration. Au contraire. Avec un nombre de foyers équipés de plus en plus important, avec des entreprises parfois dépassées par les enjeux de la sécurité, avec des méthodes d'attaques de plus en plus complexes et efficaces, et avec des réseaux de pirates toujours plus grands, il y a effectivement de quoi s'inquiéter. On le sait, le temps des virus programmés à la gloire des pirates est de l'histoire ancienne. Aujourd'hui, vers, virus, spam, phishing ou pharming n'ont qu'un seul objectif: l'argent. D'ailleurs, pour la première fois, la cybercriminalité a généré cette année plus d'argent que le trafic de drogues (voir notre article). **Menaces combinées** Surtout, comme le souligne Dave Rand, Chief Technologist of Internet Content Security (CTICS) chez Trend Micro, *« les attaques actuelles utilisent tout l'éventail de techniques possibles, et tous les moyens de distribution. Les menaces combinées constituent désormais le premier type d'attaque dans le monde. Car elles sont très efficaces »*. Par ailleurs, les menaces ne se contentent plus du monde de l'ordinateur en tant que tel. *« Nous observons la montée en puissance des menaces visant les périphériques comme les imprimantes reliées à un serveur d'entreprise et aussi les terminaux mobiles de plus en plus perfectionnés donc faillibles »*, ajoute le CTICS. Mais selon Trend Micro, la véritable menace vient de l'amélioration des techniques de botnet (réseaux de machines zombies) et du phishing. Les réseaux botnet sont des ensembles d'ordinateurs infectés pilotés à distance par un botmaster. Ces machines servent ensuite à distribuer des attaques par deni de service (DDoS) qui paralysent des sites internet. Les objectifs sont variés: faire tomber un concurrent en saturant sa plate-forme en ligne ou rançonner une entreprise. **Botnet plus faciles** Trend Micro souligne que ces attaques sont en forte augmentation et concernent de plus en plus de machines qui sont infectées à l'insu de leurs utilisateurs. Le succès de l'informatique dans les foyers depuis quelques années n'y est pas étranger. Surtout, elles sont de plus en plus efficaces. Selon honeynet.org, il suffit désormais de 13 machines zombies pour faire tomber un site. Or la moyenne des botnet est de 2.000 machines ! Et le plus grand réseau de botnet observé compte pas moins de 226.585 machines ! Par ailleurs, les méthodes de pilotage des botnet ont fortement évolué. Au départ, tout se passait au sein des chaînes IRC. Ensuite, ces chaînes ont été camouflées le plus possible. Aujourd'hui, Trend Micro souligne l'émergence de consoles et serveurs Web de C&C (Command and Control). En clair, ces outils, qui se présentent sous la forme d'interfaces graphiques, sont beaucoup plus faciles à utiliser. Lorsqu'il fallait mettre les mains dans le cambouis dans IRC, ces nouveaux outils permettent à des personnes moins calées de mettre en place des réseaux de machines zombies. La simplification des techniques et des échanges d'infos, combinés à l'appât du gain font que la menace est chaque mois plus importante, s'inquiète l'éditeur. **Mono-culture** Évidemment, la mono-culture du monde informatique autour de Windows augmente l'ampleur du problème. En cas d'incendie, une forêt hétérogène brûlera toujours moins vite qu'une

forêt composée que d'un seul type d'arbre, explique Trend Micro. Quant au phishing, véritable star de l'année 2005, sa montée en puissance est exponenentielle. 4,5 millions de mails exploitant le phishing ont été repérés en novembre 2005 contre 2,5 millions en juillet et 337.000 en janvier… Là encore, les techniques s'améliorent, les attaques deviennent ciblées avec des messages écrits dans la langue de l'internaute. Combiné aux autres techniques d'attaques, le phishing devrait encore monter en puissance, prévient Trend Micro. Aux banques et aux sites internet de réagir, de proposer par exemple l'authentification forte. Mais seule la moitié du chemin sera faite. L'éditeur souligne l'importance de la responsabilisation des utilisateurs, notamment en entreprise. *« Souvent, l'utilisateur pense que la sécurité est l'affaire du responsable informatique. Non, c'est l'affaire de tous. Business et sécurité doivent aujourd'hui être indissociables »*, conclut Dave Rand.