La menace des attaques 'zero-day' a progressé en 2006

Selon le rapport annuel du SANS intitulé Top 20 Security Attack Targets, les pirates exploitent de plus en plus les vulnérabilités inconnues dites *« zero-day flaws »* et s'attaquent à une gammes d'applications de plus en plus vaste.

La menaces des *« exploits zero-day?* est en constante progression. Il s'agit d'un programme qui permet d'exploiter une faille d'un système qui n'a pas encore été détectée ou récemment découverte mais dépourvue de patches. Logiquement, les logiciels de sécurité parviennent rarement à les détecter. D'où la redoutable efficacité de ce type « d'exploits » pour endommager des systèmes et à installer des programmes malveillants.

Si Internet Explorer demeure encore et toujours la cible privilégiée, on observe aujourd'hui une diversité des attaques qui tendent à cibler d'autres applications. Selon les observations du groupe d'experts en sécurité, le nombre d'attaques affectant Microsoft Office a triplé au cours de l'année 2006. L'éditeur a annoncé environ 45 vulnérabilités sous Office classées comme sérieuses ou critiques. Neuf de ces vulnérabilités ont été présentés comme des « exploits zero-day » actifs.

Cette année, Excel et PowerPoint se sont révélés les cibles favorites des pirates pour la suite Office. Une augmentation importante du nombre de vulnérabilités signalées a été en effet observée pour les deux produits. SANS attribue cette hausse en partie à la prévalence d'Office et au fait que la suite bénéficie d'une protection inférieure à celle des autres programmes tels que les navigateurs Web, par exemple.

Le rapport fait état également d'une recrudescence des attaques dirigées contre deux technologies émergentes : la VoIP et les Web applications. La technologie de téléphonie sur Internet est devenue l'année dernière une source d'inspiration pour les pirates, qui ont commencé à pénétrer dans les réseaux VoIP et à revendre des minutes volées à des clients ignorant tout de la ma n?uvre.

SANS pense également que les systèmes VoIP infectés pourraient être utilisés pour lancer une attaque par déni de service contre des systèmes téléphoniques traditionnels comme les réseaux RTC. Quant aux applications Web telles que les sites de commerce électronique ou de banque en ligne, elles constituent également des cibles de choix. En exposant les bases de données sur le Web, les entreprises prennent le risque de piratage en facilitant l'accès à des informations d'accès confidentielles.

Pour finir, le rapport attribue plusieurs millions de cas de vol de numéros de cartes de crédit à des attaques dites par injection SQL et de *Cross Site Scripting*. Selon un projet de test interne au SANS, 40% des applications Web vérifiées étaient vulnérables à une attaque par injection SQL et 80% à des attaques de type CSS.