‘Les chevaux de Troie bancaires évoluent’ avertit PandaLabs

20% des chevaux de Troie détectés par l’analyseur en ligne Panda ActiveScan en 2006 étaient de type bancaire. PandaLabs met en garde contre l’évolution rapide des chevaux de Troie bancaires. Ces malwares sont conçus pour dérober des informations financières.

Un exemple récent, le cheval de Troie StealAll.A injecte une DLL dans le navigateur Internet pour dérober les données entrées par les utilisateurs dans les formulaires en ligne.

Selon PandaLabs, **53,6%** des nouveaux malwares apparus en 2006 étaient des chevaux de Troie. Les chevaux de Troie bancaires ont représenté **20%** de l’ensemble des chevaux de Troie détectés par Panda ActiveScan en 2006. Il s’agit du type de cheval de Troie le plus détecté l’année passée.

La rapide évolution des chevaux de Troie bancaires est en grande partie due aux mesures de sécurité supplémentaires entreprises par les banques et autres institutions financières, notamment l’utilisation de claviers virtuels pour empêcher les enregistreurs de frappes traditionnels d’enregistrer les touches entrées par les utilisateurs.

Cependant, les cyber-escrocs redoublent d’efforts pour contrecarrer ces nouvelles mesures de sécurité. Quelques mois auparavant, PandaLabs a détecté un cheval de Troie bancaire, **Banbra.DCY**, qui est conçu pour effectuer des captures vidéo afin de visualiser les mots de passe entrés dans les champs de saisie des formulaires à l’aide d’un clavier virtuel.

Rappelons que le pharming est une autre des techniques couramment utilisées par les chevaux de Troie. Cette attaque consiste à détourner le DNS, le système qui associe les noms de domaines avec leur adresse numérique.

Ainsi lorsque les utilisateurs essaient de se connecter au site de leur banque, le cheval de Troie les détourne vers un site contrefait afin de récupérer leurs données personnelles. Banker.CHG est un exemple typique de cheval de Troie utilisant des techniques de pharming.

« Les chevaux de Troie bancaires sont actuellement une des plus grandes menaces sur Internet. Les attaques avec ces codes malicieux peuvent avoir de graves conséquences financières pour les utilisateurs. », explique Luis Corrons, le directeur technique de PandaLabs, qui ajoute : *« Ces chevaux de Troie sont créés spécifiquement pour s’installer et agir sans attirer l’attention des utilisateurs. Pour cette raison, ils ont besoin de technologies de protection proactives capables de détecter les nouvelles menaces grâce à l’analyse comportementale. »*