Un nouveau Cheval de Troie s'attaque à MacOS

Il y a moins d'une semaine, SecureMac lançait une alerte concernant un trojan impactant les utilisateurs des 10.4 et 10.5 du système d'exploitation d'Apple. Le canasson était plutôt dangereux puisqu'il permettait entre autres de voler moult informations personnelles.

Ce jeudi, c'est Intego qui tire la sonnette d'alarme après avoir repéré un nouveau cheval de Troie appelé 'PokerGame'. Il est distribué par mail sous la forme d'un ficher compressé (.zip). Evidemment, avec un nom pareil, les auteurs de ce malware comptent surfer sur la popularité de ce jeu sur la planète. Il touche les versions 10.4 et 10.5 de MacOS X.

Néanmoins, pour être infecté, il faut le vouloir. Exécuté, le fichier demande le mot de passe administrateur de l'utilisateur. Si celui-ci est donné, le trojan ouvre alors une SSH (secure shell) qui établit une liaison avec un serveur distant. Une SSH permet en effet d'échanger de façon « sécurisée » des données entre deux machines.

Une fois la communication établie, le malware envoie login-in et mots de passe, ainsi que l'adresse IP du Mac infecté. A partir de ce moment, le pirate a les mains libres pour prendre à distance et intégralement le contrôle de la machine.

'PokerGame' serait apparu sur les réseaux vendredi dernier. Il serait distribué à partir d'un site Web de hackers et on le trouve également sur iChat (messagerie instantanée) et LimeWire (service P2P).

Décidément, le succès de MacOS X a son revers...