

Mac OS X sous la menace d'un dangereux cheval de Troie

Flashback n'est pas un inconnu. Ce *malware* est un cheval de Troie qui exploite des vulnérabilités de Java afin de s'installer sur un Mac. Jusqu'à présent, Flashback avait besoin de la complicité inconsciente d'un internaute en visite sur un site vérolé pour transiter vers sa machine. Une fois installé, Flashback télécharge et installe du code malicieux et un *key logger* (enregistreur de frappe) qui vient *sniffer* (aspirer) les noms et mots de passe saisis lors d'une transaction sur un site web, comme Paypal ou la saisie des identifiants d'une carte bancaire.

Flashback.G complexifie la menace

Avec Flashback.G, nouvelle variante sophistiquée du cheval de Troie, la situation devient critique. En effet, le *malware*, qui continue d'exploiter deux vulnérabilités de Java découvertes en 2008 et l'an passé, s'installe et s'exécute seul. Les failles ont été corrigées avec les mises à jour de Mac OS X en novembre dernier, mais comme d'habitude seules les personnes qui ont fait l'effort d'effectuer la mise à jour sont à l'abri de la menace.

Rappelons que Java n'est plus livré avec Mac OS X depuis la version 10.7 Lion (lancée en juillet 2011), que l'utilisateur qui souhaite exécuter un programme Java est invité à télécharger l'environnement, et que pour le moment Apple assure les mises à jour avec celles de son OS.

Cette information est l'occasion de rappeler que le Mac d'Apple est aussi la cible des *hackers* mafieux et que la réputation sécuritaire de l'Unix embarqué comme OS du Mac ne le met pas à l'abri des menaces, alors que nombre d'utilisateurs des produits de la pomme continuent d'affirmer que le système suffit à les protéger.