

# Un cheval de Troie s'immisce dans Mac OS

## X

A mesure que la part de marché de Mac OS X progresse, les problèmes de sécurité se multiplient. SecureMac lance ainsi une alerte concernant un cheval de Troie impactant les utilisateurs des 10.4 et 10.5 du système d'exploitation. La sale bête est diffusée à travers les réseaux iChat et Limewire.

Il prend la forme d'une application ou d'un script compilé. Il peut se nommer **ASthtv05 (60 Ko) ou AStht\_v06 (3,1 Mo)**. Le canasson exploite une faille critique du système située dans Apple Remote Desktop. Si l'utilisateur exécute le dit fichier, le script obtient les privilèges administrateurs, s'installe dans le système et s'exécute à chaque démarrage. Il neutralise les messages systèmes et ouvre les port du *firewall*.

Ce n'est pas tout, le Troyen est également doté d'un *keylogger* qui enregistre vos frappes au clavier, active le partage de fichier, prend des captures d'écran, transmet les mots de passe... Bref, les risques sont très nombreux.

En attendant le correctif d'Apple, certains anti-virus dédiés (comme Intego et SecureMac) ont été mis à jour pour se protéger de cette faille. Il est également possible d'activer manuellement la gestion à distance ce qui a pour effet de bloquer l'exécution du script (paradoxal mais vrai). Dernier conseil : évitez de télécharger des scripts aux origines douteuses.