Une deuxième BackDoor menace les Mac

L'éditeur de solutions de sécurité informatique **Docteur Web** a découvert une nouvelle menace pour **Mac OS X**. Il s'agit d'une **BackDoor**, c'est à dire un malware utilisé pour prendre le contrôle d'un ordinateur à l'insu de son utilisateur.

Jusqu'à présent il n'en existait qu'un seul visant aussi bien les machines de la firme de Cupertino que celles sous Windows: le BackDoor.DarkHole. Ce virus, une fois dans le système **permet au pirate d'utiliser à distance un ordinateur**. Il peut ainsi ouvrir des pages web dans le navigateur, redémarrer l'ordinateur ou effectuer quelques manipulations avec les fichiers existants.

Aujourd'hui le nouveau venu découvert par Docteur Web se nomme **BackDoor.Olyx.** Il s'introduit dans la machine sous la forme d'une application Mac OS dont l'architecture est compatible avec les processeurs Intel dont sont dotés les machines de Cupertino.

D'après l'éditeur de sécurité russe, ce malware *«installe sur le disque un dossier /Library/Application Support/google/, sur lequel il crée un fichier appelé startp. Ensuite, le BackDoor.Olyx place le fichier /Library/LaunchAgents/www.google.com.tstart.plist dans le répertoire / home, et l'utilise pour lancer l'objet malveillant après le redémarrage de la machine».* Et de poursuivre : «*Le programme se place lui-même dans un dossier temporaire appelé google.tmp pour supprimer le fichier exécutable de son emplacement initial. Le BackDoor.Olyx opère dans un système infecté en téléchargeant et lançant des fichiers malveillants et en exécutant des commandes dans le /bin/bash shell.»*

Grâce à ce processus **le hacker contrôle donc l'ordinateur** sans que son utilisateur ne puisse s'en rendre compte à première vue. Une nouvelle preuve que les Mac peuvent être infectés. Et aussi vite désinfecté grâce aux outils de Dr Web, notamment, puisque BackDoor.Olyx est désormais enregistré dans sa base virale.