Apple réagit face au cheval de Troie MacDefender

Le cheval de Troie **MacDefender** a fait son apparition sur Mac OS X il y a de cela quelques semaines. C'est précisément le 2 mai qu'Intego, éditeur français de logiciels de sécurité Internet et de protection de données pour Mac OS X, l'a découvert. Il s'agit bien d'un cheval de Troie (*trojan*) et non d'un malware de type phishing (hameçonnage) ou encore d'un virus (il ne se reproduit pas de lui-même). Afin de ne pas l'installer sur votre machine, il convient de comprendre comment MacDefender se présente.

C'est en allant sur certains sites Internet que vous ferez sa rencontre. Une aide vous sera alors proposée pour effacer un prétendu virus qui aurait infecté votre système d'exploitation. Et **c'est précisément en acceptant cette 'aide' que vous installerez le *trojan* MacDefende**r (qui peut également se présenter sous d'autres noms : MacSecurity ou encore MacProtector) si votre Mac tourne sous Mac OS X (10.4, 10.5 ou 10.6 selon le support d'Apple). Les hackers ont de surcroît utilisé des techniques de SEO (optimisation dans les moteurs de recherche) afin de positionner les sites malveillants qui l'exploitent en tête de nombreux résultats de recherche.

Dès lors, **des fenêtres de type pop-up à caractère pornographique apparaîtront sporadiquement sur votre écran** et malveillance ultime, vous serez invité à payer l'aide offerte par cet «anti-virus» en donnant votre code de carte bleue. Les consignes d'Apple pour éviter d'installer malencontreusement ce *malware* ou bien pour l'effacer se trouvent sur le site du support d'Apple. Quant à la mise à jour de Mac OS X, elle détectera automatiquement MacDefender et l'effacera. Elle avertira également les utilisateurs lorsque ceux-ci seront sur le point de télécharger le cheval de Troie.

MacDefender n'est pas le premier, ni le dernier, agent malveillant à sévir sur Mac OS X. On pense à AppleScript.THT (2008) et plus récemment à Boonana (octobre 2010). C'est le succès d'un système d'exploitation qui fait qu'il est plus ou moins «convoité» par les hackers. On le voit avec l'OS mobile Android de plus en plus victime de chevaux de Troie, virus et autres escroqueries à l'hameçonnage.

Apple réagit un peu tardivement (MacDefender est arrivé il y a plusieurs semaines) mais a le mérite de prendre des mesures eu égard au nombre de machines infectées (plus de 120.000). On notera toutefois que les termes employés par Apple dans ses consignes sont fallacieux puisqu'il ne s'agit pas de phishing (hameçonnage) même si MacDefender appâte l'utilisateur pour mieux le tromper.