Intego Security Alert

Published on 11/02/07

A malicious Trojan Horse has been found on several pornography web sites, claiming to install a video codec necessary to view free pornographic videos on Macs. A great deal of spam has been posted to many Mac forums, in an attempt to lead users to these sites. OSX.RSPlug.A Trojan Horse Changes Local DNS Settings to Redirect to Malicious DNS Servers.

Description: A malicious Trojan Horse has been found on several pornography web sites, claiming to install a video codec necessary to view free pornographic videos on Macs. A great deal of spam has been posted to many Mac forums, in an attempt to lead users to these sites.

Exploit: OSX.RSPlug.A Trojan Horse

Discovered: October 30, 2007

Risk: Critical

When the users arrive on one of the web sites, they see still photos from reputed porn videos, and if they click on the stills, thinking they can view the videos, they arrive on a web page that says the following:

Quicktime Player is unable to play movie file.
Please click here to download new version of codec.

After the page loads, a disk image (.dmg) file automatically downloads to the user's Mac. If the user has checked Open "Safe" Files After Downloading in Safari's General preferences (or similar settings in other browsers), the disk image will mount, and the installer package it contains will launch Installer. If not, and the user wishes to install this codec, they double-click the disk image to mount it, then double-click the package file, named install.pkg.

If the user then proceeds with installation, the Trojan horse installs; installation requires an administrator's password, which grants the Trojan horse full root privileges. No video codec is installed, and if the user returns to the web site, they will simply come to the same page and receive a new download.

This Trojan horse, a form of DNSChanger, uses a sophisticated method, via the scutil command, to change the Mac's DNS server (the server that is used to look up the correspondences between domain names and IP addresses for web sites and other Internet services). When this new, malicious, DNS server is active, it hijacks some web requests, leading users to phishing web sites (for sites such as Ebay, PayPal and some banks), or simply to web pages displaying ads for other pornographic web sites. In the first case, users may think they are on legitimate sites and enter a user name and password, a credit card, or an account number, which will then be hijacked. In the latter case, it seems that this is being done solely to generate ad revenue.

Under Mac OS X 10.4, there is no way to see the changed DNS server in the operating system's GUI. Under Mac OS X 10.5, this can be seen in the Advanced Network preferences; the added DNS servers are dimmed, and cannot be removed manually. (Intego is currently testing previous versions of Mac OS X; it is likely that they can be infected as well, since all versions of Mac OS X have the scutil command.)
The Trojan horse also installs a root crontab which checks every minute to ensure that its

DNS server is still active. Since changing a network location could change the DNS server, this cron job ensures that, in such a case, the malicious DNS server remains the active server.

This Trojan horse also provides different versions of itself, perhaps according to the country in which the user is located to provide country-specific spoofing. Repeated downloads of the disk image show that there are several different versions.

Means of protection: The best way to protect against this exploit is to run Intego VirusBarrier X4 with its virus definitions dated October 31, 2007. Intego VirusBarrier X4 eradicates the malicious code and prevents the Trojan horse from being installed. Intego recommends that users never download and install software from untrusted sources or questionable web sites.

Website:
http://www.intego.com

Intego develops and sells desktop Internet security and privacy software for Macintosh. Intego provides the widest range of software to protect users and their Macs from the dangers of the Internet. Intego's multilingual software and support repeatedly receives awards from Mac magazines, and protects more than one million users in over 60 countries. Intego has headquarters in the USA, France and Japan. As the dangers of the Internet grow, Intego is hard at work, developing new software to protect users and their Macs from the latest security and privacy threats. We protect your world.

###

Rosaline Mills
PR Consultant
+44 (0)845 2577115

rosaline@bamboopr.co.uk

****
Link To Article: https://prmac.com/release-id-1002.htm
****