

20 June 2008

By: Filip Truta, Apple News Editor



[It's Official: Mac Trojan on the Loose](#)

As many as three security firms have acknowledged the threat so far

Well, it seems the guys behind [iAntiVirus](#) and [VirusBarrier X5](#) knew what they were talking about. Makers of Mac anti-spyware and anti-virus solutions, SecureMac, have discovered what is reported as a new Mac OS X Trojan horse. Dubbed "Applescript.THT Trojan," the malware is thought to have originated via a "hacker" website, Limewire and even Apple's own iChat.Applescript.THT Trojan is disguised as an application bundle called 'Astht_v06' weighing in at 3.1MB in size, macnn is reporting.From [SecureMac](#): *SecureMac has discovered multiple variants of a new Trojan horse in the wild that affects Mac OS X 10.4 and 10.5. The Trojan horse is currently being distributed from a hacker website, where discussion has taken place on distributing the Trojan horse through iChat and Limewire.* According to SecureMac, the Trojan horse runs hidden on the system, and allows a malicious user complete remote access to it. The malware can send system and user passwords, and can avoid detection by opening ports in the firewall and turning off system logging. Even worse, the AppleScript.THT Trojan horse can log keystrokes, take pictures with your Mac's built-in iSight camera, take screenshots of whatever you are doing at a given moment, and even turn on file sharing, exposing your personal life even more.Earlier today, we reported that security firm Intego claimed to have found a new vulnerability connected to Remote Management in Mac OS X. The company is also offering a solution for this - its VirusBarrier X5 for Mac OS X 10.5.2 (Leopard). The recently discovered vulnerability with the Apple Remote Desktop Agent, which allows it to run as root, is exactly what the Trojan horse exploits. SecureMac warns that the malware is distributed as either a compiled AppleScript - ASthtv05 (60 KB in size), or as an application bundle - AStht_v06 (3.1 MB in size).However, the user must download and open the Trojan horse in order to become infected. It moves itself immediately to the /Library/Caches/ folder and adds itself to the System Login Items, according to SecureMac. This is where the company's MacScan 2.5.2 comes in and saves the day. MacScan detects, isolates, and removes spyware like applications, such as keystroke loggers and Trojan horses, to protect your Mac.[Here's](#) a trial version of the software. Whether you're planning on installing security software on your Mac, the best thing you can do is never download and install software from untrusted sources or dubious websites.