

23 June 2008

By: Filip Truta, Apple News Editor



[Confirmed: Reported Mac OS X Trojan Is a Poker Game](#)

'OSX.Trojan.PokerStealer' is the official name of the Mac Trojan

Towards the end of last week the Mac-based web was "infected" with news of a [Mac Trojan](#) that will allegedly let hackers run code "as root" on other folks' machines. As usual, users would have to download and install an app - which has been confirmed as OSX.Trojan.PokerStealer, [according](#) to TUAW - in order to let hackers gain root privileges to their system. Last week, security firm Intego claimed to have found a vulnerability connected to Remote Management in Mac OS X. The company was quick to offer a solution (no surprise there), namely its VirusBarrier X5. Mac OS X Leopard users may have a look at some of its features right [HERE](#). Intego noted that the ARDAgent is owned by root. Since running code through the ARDAgent executable is done as root, it will not require a password. "When an application enables a root privilege escalation of this type, any malicious code that is run may have devastating effects," Intego warns. "A vulnerability has been discovered that allows malicious programs to execute code as root when run locally, or via a remote connection, on computers running Mac OS X 10.4 and 10.5," Intego further states. "This vulnerability takes advantage of the fact that ARDAgent, a part of the Remote Management component of Mac OS X 10.4 and 10.5, has a setuid bit set. Any user running such an executable gains the privileges of the user who owns that executable. In this case, ARDAgent is owned by root, so running code via the ARDAgent executable runs this code as root, without requiring a password. The exploit in question depends on ARDAgent's ability to run AppleScripts, which may, in turn, include shell script commands," the security firm explains. The exploit reported by Intego depends on the ability of the ARDAgent to run AppleScripts. This may, in turn, include shell script commands. The company says "the best way to protect against this exploit is to run Intego VirusBarrier X5 with its virus definitions dated June 19, 2008." Of course, there's always the cheap (and smart) way - just avoid downloading content from untrusted sources. The same goes with opening e-mail attachments. Adding that you now know Poker games for Mac might do you harm, you're probably still on the safe side.