

Hacker writes easy-to-use Mac Trojan

By Robert McMillan

February 25, 2011 09:30 PM ET

IDG News Service - In a sign that hackers, like everyone else, are taking an interest in everything Apple, researchers at Sophos [say they've spotted a new Trojan](#) horse program written for the Mac.

It's called the [BlackHole RAT](#) (the RAT part is for "remote access Trojan") and it's pretty easy to find online in hacking forums, according to Chet Wisniewski a researcher with antivirus vendor Sophos. There's even a [YouTube video demonstration of the program that shows you what it can do](#).

Sophos hasn't seen the Trojan used in any online attacks -- it's more a bare-bones, proof-of-concept beta program right now -- but the software is pretty easy to use, and if a criminal could find a way to get a Mac user to install it, or write attack code that would silently install it on the Mac, it would give him remote control of the hacked machine.

BlackHole is a variant of a Windows Trojan called darkComet, but it appears to have been written by a different developer. The darkComet source code is freely available, so it looks like BlackHole's author simply took that code and tweaked it so it would run on the Mac, Wisniewski said.

Mac OS X has been gaining market share on Windows lately, and that's starting to make it a more interesting platform for criminals. Wisniewski said that while Mac malware is still very rare, he has seen another Trojan, called [HellRTS](#), circulating on file-sharing sites for pirated Mac software.

Robert McMillan covers computer security and general technology breaking news for The IDG News Service. Follow Robert on Twitter at [@bobmcmillan](#). Robert's e-mail address is robert_mcmillan@idg.com

Notes: Because these articles often disappear mysteriously soon after published when it comes to the Apple OS, this is preserved on my site for historical reference.