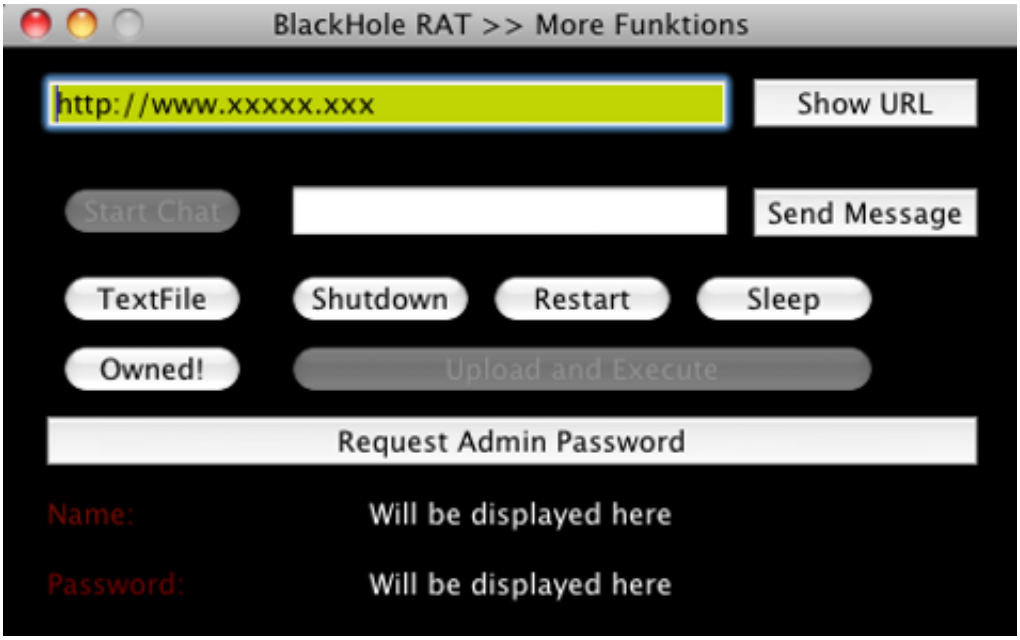
Sophos identifies a trojan for OS X

February 28 2011, by Katie Gatto



(PhysOrg.com) -- Macs have, for the most part, been considered to be more secure than their PC counterparts due to the lack of developments of viruses and other malicious codes that are created for them. Most of the authors of malicious code are playing a numbers game, in order to get the best results they need to hit the largest number of machines possible with each piece of code. As Mac operating system-based machines have become more and more popular, they have become increasingly attractive to the writers of malicious code.

A team of security researchers working at Sophos have identified a trojan that is set up to exploit a security vulnerability in Mac OSX.

The code, known as "Remote Access Trojan" or "Blackhole RAT" for short is currently unfinished, but is expected to be a Mac based version of the Windows RAT known as "darkComet". If that is the case, then Blackhole Rat will allow hackers to send commands remotely.

The commands issued from this type of trojan may give the person running the code the ability to pop up a fake "Administrator Password" window in order to perpetrate phishing styles of attack against a target. The software might also be able to be used to add files to the system, or send remote commands such as: restart, shutdown or sleep command to the Mac.

Currently the site for the trojan is very basic, with a mix of text in English and German, but the site does promise that there are upgrades to the software coming in the future. No specifics have been given, all of site would say is that "much more functions" will be released when the final product out.