'Sabpab' Trojan seeks out Mac OS X

April 17 2012, by Nancy Owano

(Phys.org) -- Three compelling reasons that Mac loyalists say justify their love for Macs have been that Macs are 1) the prettiest computers around (2) ideal for any new-age brain that prefers visually rich knowledge work and (3) their systems are far safer than Windows-based PCs, which have been sneered at as malware magnets. This year, life has got Mac-Liter as now they only have to brandish two good reasons. Researchers at major security companies such as Kaspersky Lab and Sophos say that the Mac has yet another Trojan attacker, following Flashback, that can steal information from a system once infected.

The Sabpab Trojan represents a second round of malware targeted at users of Mac machines. The earlier Flashback, according to some reports, may have succeeded in infecting as many as 600,000 Mac systems. Flashback was designed to get installed on as many machines as

possible so that its operators could profit from scams such as click fraud. Apple resolved the mess by issuing a patch while other companies offered up their own clean-up tools for detection and removal. Observers expressed concerns over how Apple was late in presenting its own tool to remove the Flashback malware, while, outside Apple, other firms had issued their free offerings.

With this latest Trojan, the exploiters are able to grab screenshots from infected Macs, upload and download files, and execute commands remotely. According to reports, the malware takes advantage of the same security flaw in Java that Flashback exploited.

Two unsettling features of the new malware are that this is a back-door Trojan that does not require any user interaction to infect and, according to Costin Rau, a security expert with Kaspersky, the Trojan is an advance persistent threat (APT) attack in an active stage.

The definition of APT varies from one security group to another, but it is not trivial. The U.S. National Institute of Standards and Technology (NIST) defines APT as “an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives” using multiple attack vectors. Mandiant, an information security company, calls the APT a sophisticated and organized cyber attack to access and steal information from compromised computers. ”The attacks used by the APT intruders are not very different from any other intruder,” says the company; the difference is in the intruder’s perseverance and resources. “They have malicious code (malware) that circumvents common safeguards such as anti-virus and they tend to generate more activity than wanton ‘drive by hacks’ on the Internet."

The APT threat is using IP addresses that have been known to wage similar attacks on Windows users, according to Kaspersky.

Sophos sources, meanwhile, say that the “Sabpab” is not believed to be as widespread as Flashback, but it is yet another wakeup call for Mac users that security is no longer a non-issue. Security on the Mac has become a key issue.