Detecting Mac OS X Trojan "Flashback"

Background

As of October 2011, a Trojan named Flashback has been targeting Mac OS X users by masquerading as a legitimate version of the Adobe Flash Player installer. Its visual elements and user interface are is quite similar, if not identical in certain cases, to the official Adobe Flash Player installer. Upon installation, it checks for the built-in Mac OS X firewall and if it is not found, the malware may request payloads from remote hosts. (1)

According to F-Secure researchers:

“There are three variants of Flashback. According to F-Secure, two of them cannot connect to their remote hosts, as they are offline. The third can connect to the remote host for additional payloads, but the host isn’t serving anything. Also, unlike the first version, the other variants are requiring an administrator password before proceeding with installation.” (2)

Mitigation Recommendations

1. It is recommended that Adobe Flash player installations only come from the official Adobe Flash website (http://www.adobe.com/products/flashplayer.html)

2. Flashback installs to “~/Library/Preferences/Preferences.dylib” so a user could check for the presence of that file to gauge whether Flashback is running on their Mac.

3. Sophos also detects the file as “OSX/FlshPlyr-A” so those with the campus-provided anti-virus software should be notified so long as their anti-virus definitions are updated. Sophos is a free anti-virus software that UCLA provides to the campus community. It can be downloaded from the UCLA Bruin OnLine Sophos website. (http://www.bol.ucla.edu/software/sophos/)

References

(1) http://www.securityweek.com/mac-os-x-trojan-targeting-apple%E2%80%99s-anti-malware-system

(2) Ibid.

Revision #16
Created Tue, Nov 1, 2011 6:13 PM by Podobas, Alexander
Updated Tue, Nov 1, 2011 6:25 PM by Podobas, Alexander