# January 2004 to September 2015

f-secure.com/weblog/archives/00002558.html

F-SECURE LABS

<<< NEWS FROM THE LAB - Wednesday, May 22, 2013 >>>

**ARCHIVES** | **SEARCH**

**Mac Spyware: OSX/KitM (Kumar in the Mac)** Posted by Sean @ 12:45 GMT

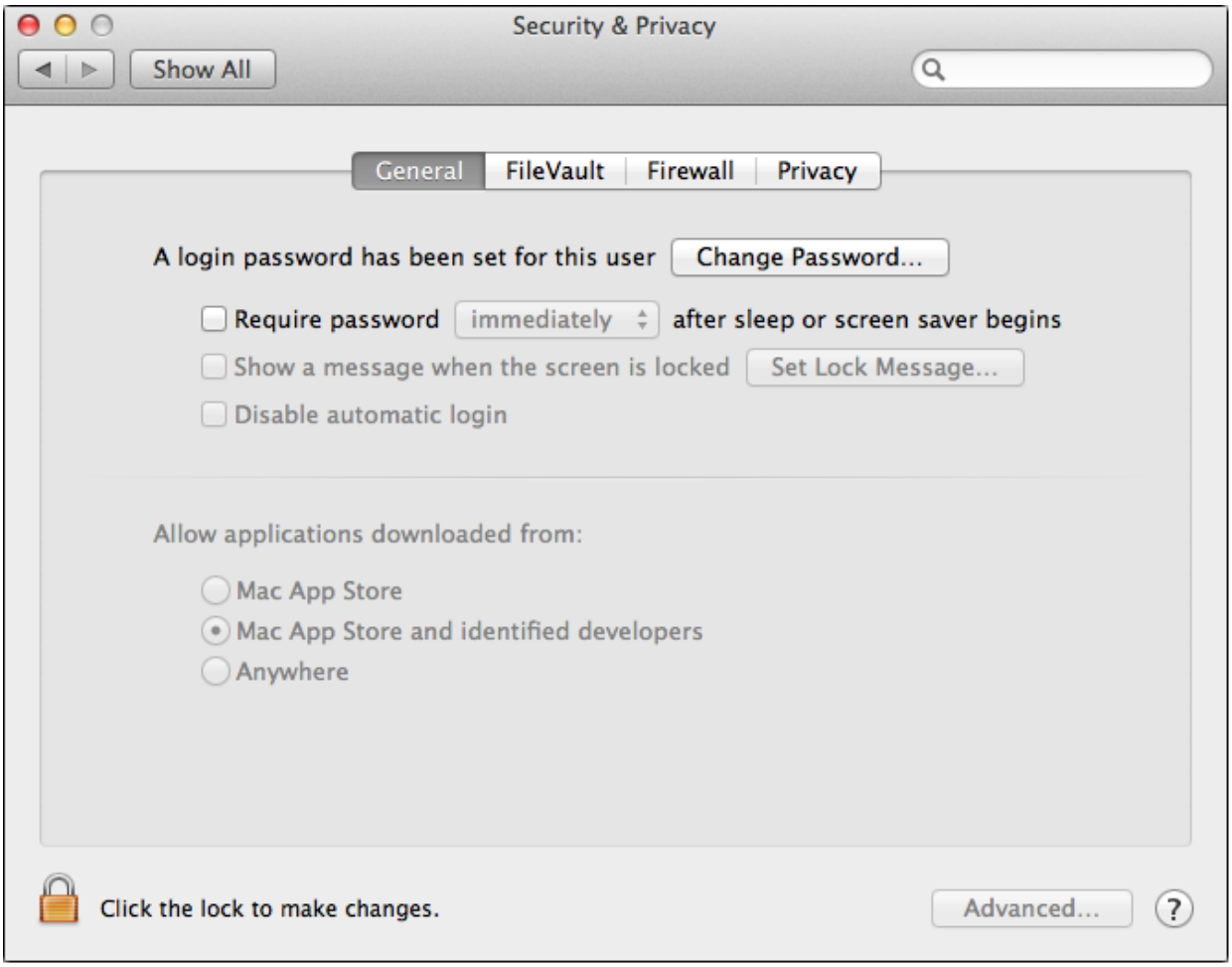
There's another case of Backdoor:OSX/KitM.A in the wild.

A German-based investigator reached out to us yesterday regarding OSX/KitM. (We wrote about it last week.) KitM stands for "Kumar in the Mac", which is our designation for spyware — related to OSX/Filesteal a.k.a. OSX/HackBack — that is signed using an Apple Developer ID in the name of Rajinder Kumar. The Developer ID has since been revoked by Apple.

This latest version of OSX/KitM used a Romanian C&C server called liveapple.eu during the period of attack, December 2012 to early February 2013. The spear phishing used an attachment called Christmas_Card.app.zip. (Remember, the attack started in December.)

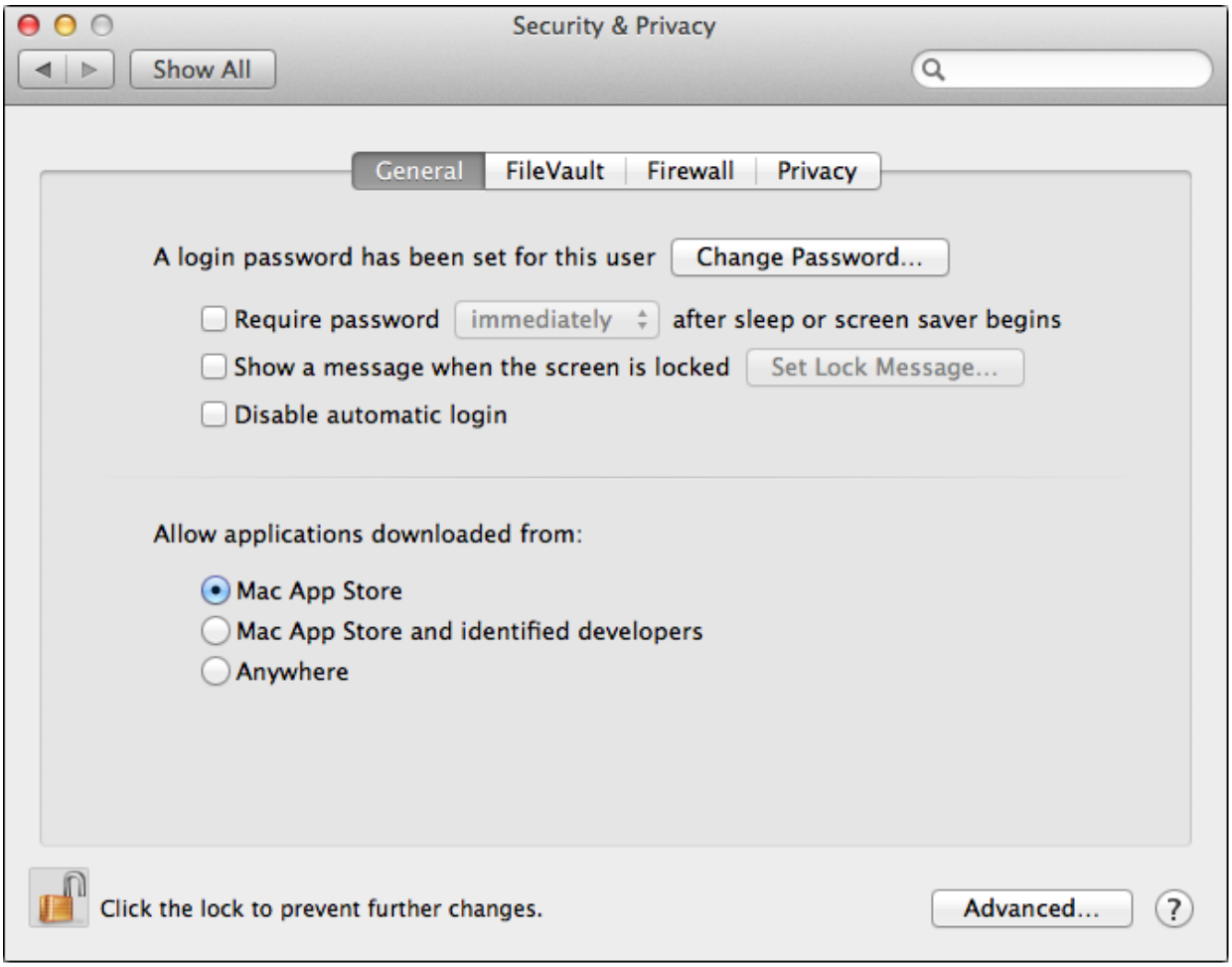
So, that brings us to this bit of advice for those of you who might be targets.

This is the default "Gatekeeper" security setting:




*Mac App Store and identified developers*

This is the setting that you want, unless you're actively installing software:




*Mac App Store*

This is the prompt that results when OSX/KitM attempts to install with the stricter setting:


If you're running OS X Mountain Lion or Lion v10.7.5 — adjust your settings as an extra layer of precaution.

SHA1: 290898b23a85bcd7747589d6f072a844e11eec65