Mac Malware Guide : How does Mac OS X protect me?

Published June 17th, 2012 at 8:31 PM EST, modified January 27th, 2013 at 11:10 AM EST (copied from www.thesafemac.com)

At this time, there is no known Mac malware that is capable of infecting a Mac running Snow Leopard (Mac OS X 10.6) or later, with a system that is kept properly updated, and with all third-party software kept properly updated, and on which certain security settings are left at their default settings. Apple has done a remarkably good job lately of keeping the system secured. There have been a number of important improvements to the system over the years.

File quarantine is a feature of Mac OS X introduced in Leopard. It is explained very well in Apple Support article HT3662, but here's the gist of it: when you download a potentially dangerous file using a quarantine-aware application (such as Safari or Mail), that file will be "quarantined." When you try to open it, the OS will warn you and ask if you really want to open it. Obviously, if you see this warning when trying to open something you didn't think was an application – for example, if you thought the file was a song in MP3 format or a picture in JPEG format – you probably shouldn't open it.

In Snow Leopard, quarantine was expanded to also check for trojans. Quarantine now uses a technology Apple has quietly named XProtect to scan downloads for known malware. The list of recognized trojans has been expanded several times from the original two (RSPlug and iServices) included in 10.6.0, and as of Security Update 2011-003, new malware definitions are downloaded daily. If you try to open a quarantined file that is actually a trojan, you will get

a very different and scarier warning that tells you the application is malware.

Example XProtect warning. Image referenced from Apple.com.

Any of Apple's applications that allow you to download support quarantine. However, results are more mixed with third-party applications. Some will support quarantine and some will not. Especially when using peer-to-peer file sharing programs, which are one of the biggest vectors for malware, I strongly advise testing support for quarantine. Download an application from a trusted source, and if you can open it without a quarantine warning, you know that the program that downloaded it does not support quarantine and could provide malware with a backdoor into your system by letting it sneak past quarantine.

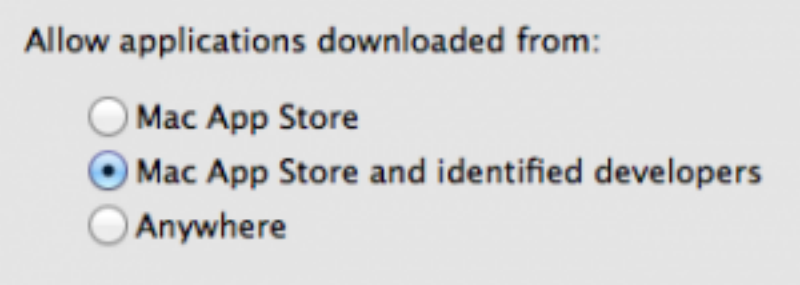
There are many web sites that will tell you how to turn these "annoying" warnings off. I strongly recommend that you do no such thing, as this can also give malware a way to sneak onto your system. Although this system has its flaws – recent variants of known trojans have proven able to slip past quarantine for a day or so, until Apple issues an

update for their malware definitions – it is nonetheless an important security feature.

The list of definitions can be found, by those interested in such things, at the following path on a Mac OS X 10.6 or 10.7 system:

```
/System/Library/CoreServices/CoreTypes.bundle/Contents/
Resources/XProtect.plist
```

If you choose Go -> Go To Folder in the Finder and paste that path into the window, that will take you there. Getting inside the CoreTypes.bundle "file" manually may be a stumper, otherwise, for those who don't know the trick.



In Mountain Lion (OS X 10.8), Apple added Gatekeeper, which provides for a way to limit what applications are allowed to run based on code signing. In System Preferences -> Security & Privacy -> General, you will see a control to set what applications are allowed, via three radio buttons. You can allow only applications downloaded from the Mac App Store, the most restrictive option. In this case, applications you downloaded from any other source will not open unless you change this setting.

You can also choose to allow applications from the App Store and those from "identified developers." This means that applications from outside the App Store will work if they have been code-signed by a developer who is registered with Apple. Code signing just means that the application has been cryptographically signed by the developer, using a key given to them by Apple. That also

means that the code cannot be modified without invalidating the signature, which in turn means that you can be sure that whatever code the app contains was written by the developer. Since developers have to pay a fee to register with Apple and get their key, it's very unlikely that such a developer would use that key to produce signed malware, and even if that did happen, Apple could quickly revoke the key, preventing the app from working further. This is probably the ideal setting for most people, since it provides a significant amount of protection without being too restrictive.

The third radio button allows you to give any application, regardless of source, the right to run. This is the same behavior as in previous systems, and you should still have XProtect defending you against known malware. However, malware has been known to get past XProtect, since XProtect – like any anti-malware software – can only protect against known threats. This is the least safe option, and I discourage its use.

Gatekeeper is integrated with the quarantine system, and thus is only capable of blocking applications that would trigger a quarantine warning (ie, those that are downloaded from the internet via quarantine-aware apps). Do not be surprised when your Gatekeeper preference does not appear to be respected for apps that were already on your machine at the time you installed Mountain Lion. For good or for ill, those apps are considered to be "trusted" apps, and will not be blocked by Gatekeeper.

It is important to understand that quarantine, XProtect and Gatekeeper **will not** protect you against Java applets that install malicious code via either Java vulnerabilities or trickery. Java provides a back door that lets that malware sneak in behind the system's back. As such, I highly

recommend disabling Java if you have it enabled, or not installing it in the first place in Lion and Mountain Lion.

If you do have Java installed, however, Apple has taken some steps to ensure that you are not in danger if at all possible. If you still have Java 6 installed, which is what is installed automatically on your system whenever you try to open a Java app, Apple has completely removed the Java web applet plug-in. This means that users of Java 6 cannot run Java applets embedded in web sites, which is the real source of concern with regard to Java. Those users do not have anything to fear from future "drive-by downloads," installed through Java vulnerabilities by an applet on a web site.

Those who have installed Java 7, downloaded from Oracle's web site, will have the Java web applet plug-in. That's a serious security risk, given how often Java vulnerabilities are discovered. Although Oracle has provided some security settings for the Java plug-in, Apple has also taken proactive measures. They will disable that plug-in if you don't use it for about a month, to protect users who simply forget they installed it and aren't using it. In addition, whenever a new Java exploit is discovered in the wild, Apple will immediately block all vulnerable versions of Java. (This doesn't always make people who rely on Java happy, but it does keep them safe.)

In addition to Java, Apple has been known to block older and insecure versions of the Adobe Flash plug-in, even though no known Mac malware has ever been installed through a Flash vulnerability.