How the Anti-Malware Function in Apple's Snow Leopard Works

Published on 09/02/09

Intego posted an article about Apple's new anti-malware function in Snow Leopard. This article provided a comparison of Apple's anti-malware function and VirusBarrier X5, and outlines some of the features that are present, or missing, in Apple's function. Now are looking at this function in more detail, describe exactly how it works, and what it does, and doesn't, do to protect Macs from malware.

Austin, TX - Since Intego posted an article about Apple's new anti-malware function in Snow Leopard, a number of sources have written about how this works. We have provided a comparison of Apple's anti-malware function and VirusBarrier X5, outlining some of the features that are present (or missing) in Apple's function. But now we'd like to look at this function in more detail, and describe exactly how it works, and what it does - and doesn't - do to protect Macs from malware.

Summary
* Apple has added an anti-malware function to Mac OS X 10.6, Snow Leopard
* This function only scans for malware in files downloaded with certain applications
* Apple's anti-malware function doesn't scan for malware when files are copied in the Finder, from CDs, DVDs, USB thumb drives or network volumes
* Apple's anti-malware function currently only scans for two Trojan horses
* Apple does not detect all variants of the most common Trojan horse
* Apple's anti-malware function doesn't scan meta-package (.mpkg) installer packages
* Apple's anti-malware function does not repair infected files or infected Macs
* Apple's anti-malware function in Snow Leopard does not offer Mac users serious protection from viruses and malware

A number of web sites have called this function "XProtect", based on the name of a file that contains information necessary to this function's operation. Apple has not given this function any "official" name, so we'll just stick with the banal "Apple's anti-malware function". The Xprotect file, called Xprotect.plist, is found in /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/; this is a more or less hidden location (it's inside CoreTypes.bundle, which is a bundle containing mostly icons).

But there's also another file in this bundle that interests us: it's called Exceptions.plist, and it contains a list of programs that are affected by Apple's anti-malware function. (We'll look closely at the contents of both of these files below.)

So, how does this function work? Apple has been using a "quarantine" function for quite some time in Safari, Mail and iChat. This function spots when files are downloaded, received as attachments to e-mail messages, or received during chats, and sets an extended attribute (data not visible to users) on such files containing information about when a file was downloaded and with which application. Here's what one extended attribute looks like for a disk image we downloaded with Safari:

com.apple.quarantine:
0000;4a9bc528;Safari.app;2E402B0A-4A8B-4E0C-B51B-47DE7BD0361E|com.apple.Safari

(Note that this extended attribute is added to all files received in the above manner, but the quarantine function only looks at certain file types, mainly executable files - applications or scripts - and installer packages.)

After mounting the disk image, if you double-click an executable file or installer package inside the disk image, the quarantine function spots the extended attribute and the system

pops up a warning.

This will also occur if you download an executable or installer package in an archive. After extracting the executable, and double-clicking it, you'll see the above warning. With malware, Apple's new function piggy-backs on this quarantine system to scan the file for malware, and, if it finds anything, the following is displayed:

What does Apple's anti-malware function scan for?

Now we get to look inside the XProtect.plist file we mentioned earlier. Looking at this file with Apple's Property List Editor, we can see that there are a grand total of two types of malware listed: the RSPlug.A Trojan horse, and the iServices Trojan horse. Intego discovered the former in October 2007 and the latter in January of this year. There are 17 variants of the RSPlug Trojan horse, and several variants of the iServices Trojan horse currently in the wild.

One interesting question is whether Apple's anti-malware function can detect all of the existing variants of the RSPlug Trojan horse. Intego's virus hunters did some tests, and found that Apple can detect only 15 of the 17 variants of the RSPlug Trojan horse. This means that two of them will get through Apple's net. It turns out that Snow Leopard does not detect the RSPlug.A nor the RSPlug.C variants. In addition, Apple's anti-malware function incorrectly identifies the variants it finds, since, in all cases, the alert displayed for any RSPlug Trojan horse variant states that the RSPlug.A variant was detected.

As for the iServices Trojan, things get a bit more complicated. This Trojan horse was found in pirated software distributed via BitTorrent sites. Yet Apple doesn't flag files downloaded with BitTorrent clients (see below). So, unless someone were to start distributing these infected disk images of iWork '09 and Photoshop CS3 via web sites, Apple's anti-malware function will never detect any iServices Trojans.

We must note a major weakness in this system. Apple's Installer uses two types of installation files: .pkg files and .mpkg files. The former are simple package files, and the latter are meta-package files, which contain several packages, often for installations that contain multiple elements. It turns out that, in our tests, Apple's anti-malware function does not spot malware contained in .mpkg files. We tested a number of RSPlug Trojan horse samples in meta-package files, and no alerts displayed. However, some of the files contained in the meta-packages, when opened on their own, set off alerts.

Which applications are protected?
We mentioned above that there's a file called Exceptions.plist that contains a list of programs that can use Apple's anti-malware function.

Under Additions you can see the identifiers of the programs that Snow Leopard currently monitors for malware. There are web browsers: Internet Explorer, Firefox, OmniWeb 5, Opera, Shiira, Mozilla Navigator and Camino; and e-mail clients: Entourage, Seamonkey and Thunderbird. (In addition to these programs are Apple's own Safari, Mail and iChat, which do not appear in the file; they have the LSFileQuarantineEnabled key set in their info.plist files. Any application that sets this key will benefit from Apple's quarantine protection, but that's up to individual developers.) Nevertheless, this doesn't apply to all types of files; for now, applications and other executables (such as scripts) are flagged, as are installer packages. Some other file types get flagged, but Trojan horses masquerading as files that are not applications can slip through the net.

Notably absent in this list are instant messaging programs (such as MSN, Adium and Skype), e-mail clients (PowerMail, Mailsmith, etc.), but above all, the vast number of applications that can download files other than from the web. No FTP programs are protected, and no BitTorrent clients or other peer-to-peer programs, both types of which are common vectors of infection.

It should be pointed out that the Finder is not protected, so files copied from network volumes or removable media (such as USB thumb drives) are not scanned at all. In addition, Apple's function can neither repair infected files, nor repair damage that may have been made if a Mac is already infected. In fact, in this latter case, Apple won't even be able to tell you that your Mac is infected.

The unknown: virus definition updates
Apple has stated that updates to the virus definition file, XProtect.plist, will be provided by its Software Update application, but not how often. To start with, only two Trojans are in the current definitions, which is far from sufficient given the extent of malware that threatens Macs. It's unclear whether Apple will wait for security updates to update that file, or whether there will be separate updates more often (Apple issues security updates for Mac OS X about ten times a year on average). Commercial antivirus software benefits from frequent updates: in Intego's case, at least twice a week, and more often when new malware or new variants are found.

Summing up
It can be seen that Apple has added a very limited anti-malware function to Snow Leopard. Not only does it only scan files from a handful of applications, and only for two Trojan horses, but it didn't even spot all the current variants that we tested. It cannot repair files or scan your Mac to find existing infections. It doesn't detect malware contained in meta-packages, making it very simple to distribute malware that will bypass Apple's protection. It cannot scan network volumes, and it won't even see infected files copied from removable media. In short, Apple's anti-malware function in Snow Leopard is notable for the lack of serious protection it provides to Mac users.

Anti-Malware Function:
http://www.intego.com/news/intego-security-memo-how-the-anti-malware-function-in-apples-snow-leopard-works.asp

VirusBarrier X5:
http://www.intego.com/virusbarrier/

Download:
https://www.intego.com/buynowUK/

Purchase:
https://www.intego.com/buynowUK/

Intego develops and sells desktop Internet security and privacy software for Macintosh. Intego provides the widest range of software to protect users and their Macs from the dangers of the Internet. Intego's multilingual software and support repeatedly receives awards from Mac magazines, and protects more than one million users in over 60 countries. Intego has headquarters in the USA, France and Japan.

###

Rosaline Mills
PR Consultant
+44 (0)845 2577115

rosaline@bamboopr.co.uk

****
Link To Article: https://prmac.com/release-id-7330.htm
****