



# The Year in Mac Security 2008

## An Annual Report from Intego

2008 was a busy year for Mac security and malware, with a number of new threats targeting Macs, from Trojan horses to scareware, from browser flaws to Mac OS X vulnerabilities. This document is a summary of the year's security issues that affected Macs. Footnotes link to articles on the Intego Mac Security Blog (<http://blog.intego.com>) with further information about these issues.

### Trojan Horses

Intego first discovered the RSPlug Trojan horse in October 2007<sup>1</sup>, and since that time, a number of variants have been found in the wild, and more and more Mac users have been infected by these malicious programs.

In April of this year, Intego reported<sup>2</sup> on a number of new variants of this Trojan horse that had been found. Most of the variants weren't really variants; but were simply disk images with different names from the original. (One antivirus vendor claimed to have found some three dozen such variants, but did not, it seems, examine the code to see that they were all the same.)

Other variants include two whose code was different, but some variants purported to install differently-named software. The original RSPlug Trojan horse installed "software" called MacCodec; other versions' installers claim to install MacVideo or Porn4Mac. Also, the containers—the disk images containing the installers—differ. The first version was found in a series of disk images named with four digits followed by the disk image extension: for example, 1023.dmg. Others have been called operacodec1234.dmg, nitroticket2018.dmg, uincodec4264.dmg, ixcodec1292.dmg and xerocodec1292.dmg. (Note that there may be variations in the numbers contained in these names, as well as the names themselves.)

In June, Intego spotted<sup>3</sup> a new Mac OS X Trojan horse, OSX.Trojan.PokerStealer. The Trojan horse, when run, activates ssh on the Mac on which it is

running, then sends the user name and password hash, along with the IP address of the Mac, to a server. It asks for an administrator's password after displaying a dialog saying, "A corrupt preference file has been detected and must be repaired." Entering the administrator's password enables the program to accomplish its tasks. After gaining ssh access to a Mac, malicious users can attempt to take control of them, delete files, damage the operating system, or much more.

Then in November, Intego discovered another variant of the RSPlug Trojan horse, with a new twist to its actions<sup>4</sup>. While this new variant performed the same actions as the RSPlug.A Trojan horse, its installer was different: it was a downloader, which contacts a remote server to download the files it installs. This means that, in the future, the downloader may be able to install other payloads than the one it currently installs.

And when we thought we'd seen enough of RSPlug variants, another one popped up in December, this one with Intego's name on it<sup>5</sup>. This new variant, RSPlug.E, was similar to the RSPlug.D Trojan horse, but had some interesting differences with the previous versions. The samples Intego saw, named FlashPlayer.v3.348.dmg and FlashPlayer.v..dmg, contained code that referred to Intego. The actual malware code is encoded (using a standard routine called uuencode), and when it is decoded, a line of code is present saying: "begin 666 intego". This tells the system to create a file with read and write

1 <http://blog.intego.com/2007/10/31/intego-security-alert-osxrspluga-trojan-horse/>

2 <http://blog.intego.com/2008/04/11/new-variants-of-the-rsplug-trojan-horse/>

3 <http://blog.intego.com/2008/06/20/new-mac-os-x-trojan-horse-pokerstealer/>

4 <http://blog.intego.com/2008/11/18/intego-issues-security-memo-about-new-variant-of-rsplug-trojan-horse/>

5 <http://blog.intego.com/2008/12/02/yet-another-variant-of-the-rsplug-trojan-horse-this-one-taunts-intego/>

permissions (the 666 is a shortcut for Unix permissions, not anything to do with the “number of the beast”), and to create a file, containing the malicious code, named “intego”. Intego obviously had nothing to do with the creation of this malware, and felt that the choice of this file name was a provocation from the creator of this malware.

## Other Mac Malware

In November, Intego issued a security memo about a hacker tool that could be used to create Trojan horses<sup>6</sup>. Reports had been circulating about a new Mac “malware” or “Trojan horse”, usually under the name “OSX.Lamzev.A”, which was claimed to open a back door on compromised Mac OS X computers. Intego discovered this hacker tool in August 2008, and determined that it was not a serious threat. Unlike true malware and Trojan horses, this hacker tool, that we call OSX.TrojanKit.Malez, requires that a hacker already have access to a Mac in order to install the code. As of the present, no Trojan horses or other means of replication have been found in the wild using this tool. In spite of reports from other security vendors, this represents no serious threat to Macintosh computers.

This hacker tool can be used to create a “backdoor” on a Mac OS X computer. This backdoor then gives a hacker remote access to the computer. The code is added to an unsigned third-party application that is installed manually on a Mac, and, when the application is run, the backdoor is activated. It creates a file named com.apple.DockSettings in ~/Library/LaunchAgents, and the backdoor is launched at each login. The binary of the original application is placed in ApplicationName.app/Contents/MacOS/2, and the binary of the backdoor is found in ApplicationName.app/Contents/MacOS/1. The tool modifies the application’s info.plist file so it points to the latter location.

There are therefore only two modes of transmission of this hacker tool: the first is if someone sends another user an infected application, either in a .zip archive or a disk image, and the second is when a hacker obtains network access to a Mac and replaces

an existing application with an infected version.

## Scareware for Mac

The year began with a brazen attempt to scam Mac users in January by a company selling a program called Macsweeper, which claimed, “The imbibed set of features locates all the junk and useless data on your computer and deletes them to reclaim the wasted space.”<sup>7</sup> This is one of several scareware programs that was seen for Mac this year, attempting to frighten Mac users into buying bogus security software.

A clone of this program, called iMunizator, was spotted in March; it was the same program (with exactly the same interface, features and code) but with a new name. The program’s website had the same layout and the same description as Macsweeper.<sup>8</sup>

Another bogus “security” program for Mac was found in October<sup>9</sup>. MacGuard, as the program is called, claimed:

*“Macguard’s high-tech system scanner will search your hard drive for malicious objects such as Adware, Spyware and Trojans, cleaning your files, eliminating the threats, and securing your privacy in just a matter of minutes. Its Real Time smart protection will also ensure new threats will not even reach your desktop.”*

Needless to say, this was a Mac version of a common Windows scam: selling software that claims to keep you safe, but actually scams you. If you are gullible enough to purchase this software from a company you have never heard of, who has no references, and whose web site is vague and imprecise, it is likely that you will find additional charges on your credit card. One website<sup>10</sup> reported that more than 30 million people have been scammed by such software.

## Mac OS X Security Issues

While most press reports about security issues focus on malware—viruses, Trojan horses and the like—some of the more serious issues today are those related to flaws in software and in operating systems.

6 <http://blog.intego.com/2008/11/20/intego-issues-security-memo-about-a-hacker-tool-that-can-be-used-to-create-trojan-horses/>

7 <http://blog.intego.com/2008/01/15/scareware-tries-to-trick-mac-users-into-buying-worthless-software/>

8 <http://blog.intego.com/2008/03/28/new-scareware-targets-mac/>

9 <http://blog.intego.com/2008/10/17/beware-bogus-security-software/>

10 <http://arstechnica.com/news.ars/post/20081017-report-fake-antivirus-programs-claim-30-million-victims.html>

Mac OS X, while more secure than Windows, contains its share of flaws, and Apple has to constantly keep on its toes to issue a couple dozen security updates each year, to Mac OS X in general, as well as to specific parts of Mac OS X that are often found to contain vulnerabilities. Apple's not the only vendor who needs to release security updates: on the Intego Mac Security Blog we track updates to popular software such as Microsoft Office, Adobe Acrobat and Flash, and web browsers such as Firefox and Opera.

In June, Intego alerted Mac users about a critical threat in Apple Remote Desktop software<sup>11</sup>, in a module that is installed on all Macs. A vulnerability was discovered that allowed malicious programs to execute code as root when run locally, or via a remote connection, on computers running Mac OS X 10.4 and 10.5. This vulnerability took advantage of the fact that ARDAgent, a part of the Remote Management component of Mac OS X 10.4 and 10.5, had a setuid bit set. Any user running such an executable gained the privileges of the user who owns that executable. In this case, ARDAgent was owned by root, so running code via the ARDAgent executable ran this code as root, without requiring a password. The exploit in question depended on ARDAgent's ability to run AppleScripts, which may, in turn, include shell script commands.

Apple didn't issue a patch for this flaw until August<sup>12</sup>, which was one of several examples during the year 2008 of Apple taking what many commentators and researchers say is far too much time before issuing security fixes. (One such example is the several-month delay of a security patch for a DNS cache poisoning<sup>13</sup> issue that other vendors had patched months earlier.)

A serious QuickTime bug was discovered in September<sup>14</sup>, which may be a vector for future attacks. The "<? quicktime type= ?>" tag failed to handle long strings, which could lead to a heap overflow in QuickTime Player, iTunes, or any other program that attempts to display media using a QuickTime plug-in. This could be a browser, such as Apple's Safari,

Microsoft Internet Explorer or Mozilla Firefox, or, on Mac OS X, could be any program that displays graphics or movies inline, such as Mail, or even the Finder if a user tried to view a file with Quick Look. For now, files which contain offending strings will crash programs attempting to display them, but malicious code could be added to such files, and may be executed with no user interaction, other than an attempt to view a file.

Apple's Safari web browser saw a security update in November<sup>15</sup>, which added a new anti-phishing feature, called by Apple "fraudulent site" protection. Safari displays an alert when it thinks it detects a phishing site.

Apple caused a bit of a kerfuffle in late November<sup>16</sup> when the company updated a document suggesting that Macs should run antivirus software. The note said: "Apple encourages the widespread use of multiple antivirus utilities so that virus programmers have more than one application to circumvent, thus making the whole virus writing process more difficult." The note then went on to mention three antivirus programs, with Intego VirusBarrier X5 listed first.

Apple soon pulled the document, though, after many press outlets had published the information, suggesting that Mac OS X was vulnerable to malware (which, of course, it is), something that goes against Apple's marketing discourse.

Finally, in the year 2008, Apple issued 35 security updates<sup>17</sup>, for Mac OS X, QuickTime, Safari, the Apple TV, iPhoto, iLife, the iPhone and iPod touch, and much more. This represents several gigabytes of files to download, and is down just a bit from the 38 security updates the company released in 2007, though both are up sharply from the 22 security updates that were issued in 2006 and 23 in 2005. There have been far more security problems in the past two years than in previous years, requiring Mac users to be more vigilant than ever to ensure that their computers are safe and secure.

**we protect your world.**

**www.intego.com**

11 <http://blog.intego.com/2008/06/19/new-critical-threat-to-mac-os-x/>

12 <http://blog.intego.com/2008/08/01/apple-issues-important-security-update/>

13 <http://blog.intego.com/2008/07/30/more-complaints-over-apples-delayed-dns-patch/>

14 <http://blog.intego.com/2008/09/18/quicktime-bug-discovered-may-be-vector-for-attack/>

15 <http://blog.intego.com/2008/11/14/safari-update-plugs-holes-adds-anti-phishing-feature/>

16 <http://blog.intego.com/2008/11/25/apple-recommends-antivirus-software/>

17 <http://support.apple.com/kb/HT1222>