The Year in Mac Security 2010

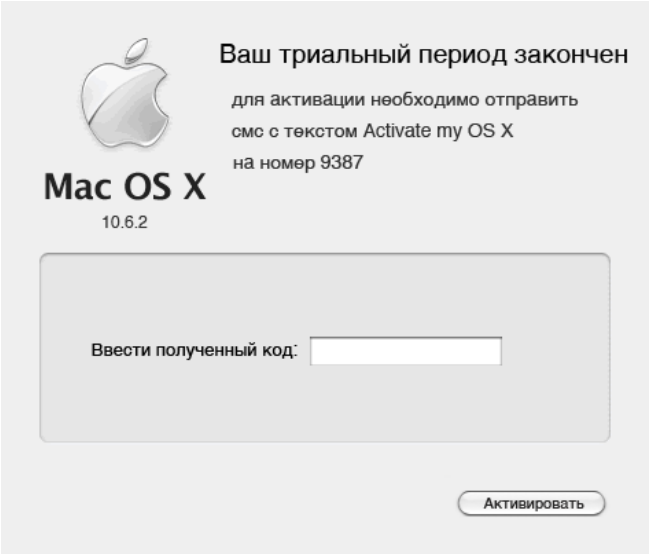
An Annual Report from Intego

2010 was another busy year for Mac security and malware, with new threats targeting Macs, security issues affecting iOS devices, and a large number of Mac OS X vulnerabilities being discovered and patched. This document is a summary of the year's security issues that affected Macs. Endnotes link to articles on the Mac Security Blog (http://blog.intego.com) which give more information about these issues.

Mac Malware

Throughout the year 2010, Intego's Virus Monitoring Center collected a large number of samples of the RSPlug malware. First discovered in October 2007[1], this DNS changing malware is a serious threat to Macs, and remains in circulation on many malicious web sites that provide access to pornography, cracked software, "free" games, "free" music and more. Many users posting to forums (including Apple's support forums) describe the symptoms of this malware, and many Mac users discover that they are infected after scanning their Macs for the first time with Intego VirusBarrier X6.

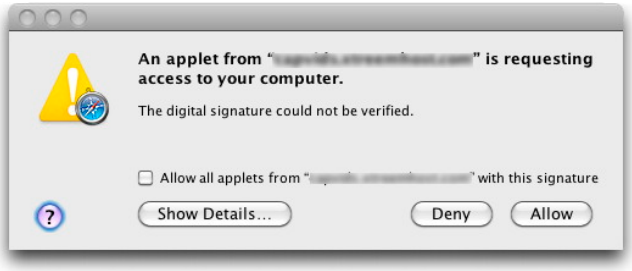
In March, a proof-of-concept ransomware for Mac OS X was shown on a couple of blogs[2]. Ransomware is malware that "locks" files, usually by encrypting them with password protection, then informs the infected user that if they want access to their files, they must pay up. This proof-of-concept was based on a feature, not a bug, in Mac OS X, and no instances of this ransomware have been found in the wild.



In April, Intego discovered a new variant of malware for Mac called HellRTS, which, when installed on computers running Mac OS X, opens a backdoor that allows remote users to take control of infected Macs and perform actions on them[3]. While this malware was distributed on a number of forums, Intego found no instances of it in the wild. Nevertheless, this type of malware can lay dormant for a long time, as malware creators develop new ways of delivering it to Mac users.

June saw the discovery of spyware affecting Mac OS X, installed by a number of freely distributed screen savers[4]. This spyware, called OpinionSpy, intended to be a tool for collecting information on users' browsing habits, was not intended to be dangerous, but many of its "features" could open backdoors, inject code into applications, and download new code without users being aware.

In October, Intego issued a security memo about a Mac version of the Koobface worm[5], which has been a serious problem for Windows users for years. This worm spreads via social networking sites, such as Facebook, Twitter and MySpace, and when users attempt to view videos, after clicking links on the aforementioned sites, the sites hosting the videos attempt to install a malicious Java applet. But the malware was anything but silent; it presented a dialog asking users if they wanted to install the applet.



While the malware itself was malicious, its code was flawed, and the threat was very low. This malware had only limited distribution, and the threat remains minimal.

Mac OS X Security Issues

Some of the more serious security issues are those related to flaws in software and operating systems. Mac OS X, while more secure than Windows, contains its share of flaws, and Apple has to constantly keep on its toes to issue several 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 issued a total of 38 security updates in 2010 for Mac OS X, Apple software and Apple hardware.

Apple's market share increased in 2010, with an estimate in March[6] suggesting that the installed base of Mac OS X was around 11% in the United States. This is naturally more than Apple's actual sales figures, but represents the fact that Mac users keep their computers longer than PC users.

Apple's first security update for Mac OS X[7], in January, fixed a number of issues, some of which were critical. Apple updated Mac OS X again in March with a huge update that patched 93 different vulnerabilities[8]; in March, an update[9] patched a bug highlighted by security researcher Charlie Miller at the Pwn2Own contest held at the CanSecWest security conference[10].

Another Mac OS X security update was issued in June[11], fixing 28 flaws; August[12] saw a Mac OS X security update patching 13 flaws; and in September, Apple issued a rare single-vulnerability security update[13] to fix a flaw in AFP (Apple Filing Protocol), the standard file-sharing protocol used in Mac OS X. Apple issued a huge security update for Snow Leopard (Mac OS X 10.6) in November[14], as well as a Leopard update at the same time[15], followed, shortly thereafter, by a Snow Leopard Server update[16].

Apple issued security updates for Java in May[17], and again in October[18], and, shortly after the latter update, Apple announced that the company was officially deprecating Java[19]: this means that, in the future, they will not be providing a Java environment with Mac OS X. Presumably, this will be available from another vendor such as Sun, but Apple has not, as yet, announced as of when they will stop shipping Java.

Apple updated its Safari web browser several times in 2010: in March[20], June[21], July[22], September[23], and again in November[24]. This said, it's fair to say that all major web browsers have security issues[25], and that Apple is not alone in updating their browser. (See below, *Third-Party Software and Macs*, for more on security updates to other browsers.)

Other Apple software updated for vulnerabilities included an update in April for AirPort base station software[26], and another in December[27]; updates to iTunes and QuickTime in March[28], another iTunes update in July[29], and a large QuickTime update in December[30].

Apple also updated their on-line MobileMe service, in May, to provide SSL access[31]. And Apple updated the software for the company's new AppleTV in November[32] to fix 8 vulnerabilities.

In January, Intego's researchers highlighted an interesting issue involving certain invisible files created by Mac OS X[33]. These files could lead to potential security issues, as they could contain lists of files in the folders where they reside. This bug has not been fixed yet.

The Mac Security Blog

Intego maintains The Mac Security Blog, which keeps Mac users up to date on the latest security threats, malware, security updates, and other security issues that affect Mac users. Found at **http://blog.intego.com**, The Mac Security Blog is updated each time new security issues arise, or when major software—both from Apple and from third parties—is updated to protect against security threats. Keep up to date on Mac security issues by visiting the blog regularly, or by subscribing to its RSS feed.

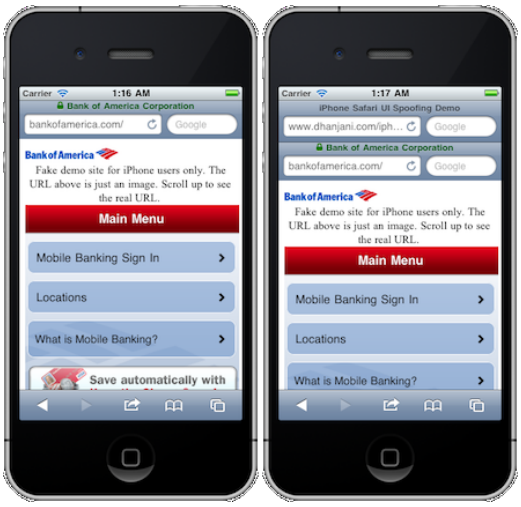
iOS Security Issues

2010 was the year of iOS, with the official name of this operating system being changed in June from iPhone OS to reflect the growing importance of the platform.

Apple issued a number of security updates to iOS: in February[34], in June[35], for a new major version of iOS, version 4, in August[36], and in September[37]. In November, Apple released iOS 4.2[38], the first iOS update for the iPad, and corrected some vulnerabilities at that time.

As iOS and other mobile platforms become ubiquitous, security and privacy issues are becoming serious issues. A Swiss security researcher made a proof-of-concept of a "rogue" iPhone app that could harvest user information in February[39]. In April, some analysts suggested that the iPad "deserves an 'F' for security readiness,[40]" but others considered that this was an exaggeration. Another researcher, in May, discovered that it was possible to access data on an iPhone from a Linux computer[41]. And in December, the Wall Street Journal[42] discovered that many popular mobile apps—both for iOS and for Android—sent personal information to advertisers.

An interesting URL hiding trick affecting iOS browsers was shown as a proof of concept in November[43]. This trick works when a web page displays a graphic of a Safari browser window, showing a fake URL. After this page has loaded, Safari's address bar disappears, leading users to believe that the URL they see in the graphic of the web page is the correct one.



Jailbreaking was also in the news. This is the process of hacking the operating system of a device to install software that is not distributed via Apple's iTunes Store, or to activate certain features that may be unavailable. In May[44], a tool was released to jailbreak the iPad, as well as other iOS devices. In July, the Library of Congress issued a statement which effectively rendered jailbreaking legal[45]. (The Library of Congress has powers over certain copyright issues.) In August, an iOS vulnerability made it possible for iOS devices to be jailbroken very easily via a web browser[46]. Apple patched this vulnerability shortly thereafter[47].

Third-Party Software and Macs

Third-party software—that from vendors other than Apple—was again the cause of much worry in 2010. Naturally, security issues go beyond malware and operating system problems, and many third-party programs are susceptible to bugs which can compromise security.

Firefox was updated 7 times for security fixes. Adobe software—especially Flash Player and Acrobat—required frequent updates, with 6 updates for Flash Player, 6 for Acrobat and 3 for Shockwave. And Microsoft Office was updated 7 times for security fixes; 6 of these updates were for Office 2004 and 2008, and one for the new Office 2011. (It's worth noting that the release of Office 2011 re-awakens an old threat to Macs via macros contained in Office documents[48]. Office 2008 had removed Visual Basic, which runs macros, but customer complaints forced Microsoft to bring back this feature in Office 2011.)

The Opera and Chrome web browsers saw security updates during the year, and Adobe released a security fix for Photoshop CS4[49], something that is not seen often.

Apple notably announced that the company was dropping Adobe's Flash Player from Mac OS X[50] in October, citing both battery life and security issues. Apple started shipping new Macs without Flash Player at the end of the year.

Other Security Issues

Many security issues are platform-independent: they rely on social engineering, or on weaknesses in protocols. The web is now a serious security threat, as social networking sites, and even standard web services, can lead to security or privacy breaches. A number of interesting issues appeared in 2010.

An interesting potential phishing trick was discovered in January. With new Internet domains able to use non-Latin characters, some letters that look like Latin characters could be used to trick users into thinking that they are on certain sites. One example[51] showing how "paypal" could be written with Cyrillic characters was especially interesting, as it would fool just about anyone who saw it.

In February, some security issues regarding Google Buzz, the company's social networking tool, were found[52]. First was the company's decision to opt all users into the service, but a cross-scripting flaw was also found in the Buzz's underlying code. And leaving Google Buzz was not very simple. Facebook changed its privacy settings in April, also making them opt-out[53], causing some consternation. In October, it was found that some Facebook apps shared confidential information about users[54].

Phishing remained an important threat. In February, one well-known netizen admitted that he fell for a phishing scam on Twitter[55]. An increasing number of phishing attempts were sent purporting to be from Apple[56]. Apple's growing market share makes these attempts more lucrative. Throughout the year, Intego saw a large number of these spams. Some interesting new Amazon phishing e-mails were also spotted in April[57]. One TV station even went as far as calling phishing e-mails an iTunes virus[58]; they've probably learned by now what phishing really is.

Google added an SSL search option to its search service in May[59]. Using the https://www.google.com address would create "an encrypted connection [...] between your browser and Google. This secured channel helps protect your search terms and your search results pages from being intercepted by a third party on your network,"Google said. Google changed the URL for secure searching in June to https://encrypted.google.com, to ensure that content filtering systems could block secure searching[60].

In May, the Electronic Frontier Foundation published some information about an experiment they had been running to see if users have unique "browser fingerprints." It turned out that they do[61], and that this information could be used to identify users even independently of cookies or other tracking methods.

An AT&T data breach affecting iPad users made a bit of noise in June[62]; this had nothing to do with the iPad itself, but rather with AT&T's database software.

A security researcher showed how it was possible to leverage data from Google Earth to locate many people based on the MAC addresses of their routers[63].

95% of all e-mail may be spam[64], though spam volume dropped drastically at the end of the year[65].

A Swiss company found a way to crack passwords at a rate of 300 billion attempts per second using SSD drives[66]. And in December, hackers obtained some 200,000 passwords and e-mail addresses from a network of popular web sites[67]. It was found that the most common password was 12345.

Conclusion

2010 was another busy year for Mac security professionals. With new malware, an extensive number of vulnerabilities affecting Mac OS X, iOS and many applications, the Mac platform saw enough security issues to keep everyone well occupied. Intego's Virus Monitoring Center recovered thousands of malware samples, and ensured that Intego's software, notably VirusBarrier X6, was always up-to-date to deal with the latest malware, web threats, phishing and more.

1 http://blog.intego.com/2007/10/31/intego-security-alert-osxrspluga-trojan-horse/
2 http://blog.intego.com/2010/03/16/mac-ransomware-threat-nothing-to-worry-about-yet/
3 http://blog.intego.com/2010/04/16/intego-security-memo-hellrts-backdoor-can-allow-malicious-remote-users-to-control-macs/
4 http://blog.intego.com/2010/06/01/intego-security-alert-osxopinionspy-spyware-installed-by-freely-distributed-mac-applications/
5 http://blog.intego.com/2010/10/27/intego-security-memo-trojan-horse-osxkoobface-a-affects-mac-os-x-mac-koobface-variant-spreads-via-facebook-twitter-and-more/
6 http://blog.intego.com/2010/03/02/mac-os-x-installed-base-nearly-11-in-us/
7 http://blog.intego.com/2010/01/20/apple-issues-security-update-patches-critical-issues/
8 http://blog.intego.com/2010/03/29/apple-releases-mac-os-x-update-with-dozens-of-security-fixes/
9 http://blog.intego.com/2010/04/15/apple-releases-security-update-patches-pwn2own-bug/
10 http://blog.intego.com/2010/03/25/hackers-crack-macs-and-others-for-cash/
11 http://blog.intego.com/2010/06/16/mac-os-x-10-6-4-update-fixes-28-security-issues/
12 http://blog.intego.com/2010/08/25/mac-os-x-security-update-fixes-over-a-dozen-flaws/
13 http://blog.intego.com/2010/09/21/apple-releases-security-update-for-afp-vulnerability/
14 http://blog.intego.com/2010/11/11/apple-releases-massive-snow-leopard-update-with-dozens-of-security-fixes/
15 http://blog.intego.com/2010/11/11/apple-releases-leopard-security-update/
16 http://blog.intego.com/2010/11/16/apple-issues-snow-leopard-server-security-update/
17 http://blog.intego.com/2010/05/19/apple-updates-java-for-10-5-and-10-6/
18 http://blog.intego.com/2010/10/21/apple-releases-java-security-updates/
19 http://blog.intego.com/2010/10/25/apple-officially-drops-flash/
20 http://blog.intego.com/2010/03/12/apple-issues-safari-security-update/
21 http://blog.intego.com/2010/06/08/apple-updates-safari-web-browser-security-fixes-included/
22 http://blog.intego.com/2010/07/28/apple-updates-safari-security-fix-included/
23 http://blog.intego.com/2010/09/08/apple-updates-safari-for-security-issues/
24 http://blog.intego.com/2010/11/18/apple-releases-large-safari-security-updates/
25 http://blog.intego.com/2010/04/29/all-major-web-browsers-have-flaws/
26 http://blog.intego.com/2010/04/01/apple-updates-airport-base-station-software-and-patches-security-flaw/
27 http://blog.intego.com/2010/12/17/apple-updates-airport-devices-and-fixes-vulnerabilities/
28 http://blog.intego.com/2010/03/31/apple-updates-itunes-and-quicktime-with-security-fixes/
29 http://blog.intego.com/2010/07/20/apple-issues-itunes-security-update/
30 http://blog.intego.com/2010/12/08/15-vulnerabilities-patched-in-apples-latest-quicktime-update/
31 http://blog.intego.com/2010/05/21/apple-updates-mobileme-making-it-more-secure/
32 http://blog.intego.com/2010/11/22/apple-releases-apple-tv-update-with-security-fixes/
33 http://blog.intego.com/2010/02/11/possible-security-issue-involving-ds_store-files-on-web-servers/
34 http://blog.intego.com/2010/02/03/apple-issues-security-update-for-iphone-os/
35 http://blog.intego.com/2010/06/22/apple-updates-ios-patches-holes-fixes-flaws-squashes-bugs/
36 http://blog.intego.com/2010/08/12/apple-updates-ios-fixes-jailbreak-vulnerability/
37 http://blog.intego.com/2010/09/09/ios-update-features-several-security-fixes/
38 http://blog.intego.com/2010/11/22/apple-releases-ios-4-2-with-many-security-fixes/
39 http://blog.intego.com/2010/02/04/should-iphone-users-worry-about-rogue-apps/
40 http://blog.intego.com/2010/04/21/is-the-ipad-secure-enough-for-businesses/
41 http://blog.intego.com/2010/05/27/iphone-data-vulnerability-access-iphone-data-from-linux-computer/
42 http://blog.intego.com/2010/12/20/many-iphone-apps-send-personal-info-to-advertisers/
43 http://blog.intego.com/2010/11/30/researcher-points-out-url-hiding-trick-on-iphone/
44 http://blog.intego.com/2010/05/04/ipad-iphone-jailbreak-tool-available/
45 http://blog.intego.com/2010/07/27/jailbreaking-an-iphone-is-now-officially-legal-in-the-us/
46 http://blog.intego.com/2010/08/04/ios-vulnerability-allows-web-based-iphone-jailbreak/
47 http://blog.intego.com/2010/08/12/apple-updates-ios-fixes-jailbreak-vulnerability/
48 http://blog.intego.com/2010/10/15/microsoft-office-2011-and-macros/
49 http://blog.intego.com/2010/05/27/adobe-issues-security-update-for-photoshop-cs4/
50 http://blog.intego.com/2010/10/25/apple-officially-drops-flash/
51 http://blog.intego.com/2010/01/04/non-latin-domain-names-could-raise-new-phishing-issues/
52 http://blog.intego.com/2010/02/17/google-buzz-has-multiple-security-issues/
53 http://blog.intego.com/2010/04/27/facebooks-new-privacy-settings-are-opt-out/
54 http://blog.intego.com/2010/10/18/facebook-apps-share-confidential-user-information/
55 http://blog.intego.com/2010/02/24/twitter-phishing-scam-traps-savvy-netizen/
56 http://blog.intego.com/2010/03/25/apple-store-spam-proliferates/
57 http://blog.intego.com/2010/04/24/new-type-of-amazon-com-phishing-e-mail/
58 http://blog.intego.com/2010/10/05/itunes-virus-hold-everything/
59 http://blog.intego.com/2010/05/22/google-adds-ssl-search-option-for-search-data-security/
60 http://blog.intego.com/2010/06/29/google-changes-secure-search-url/
61 http://blog.intego.com/2010/05/18/you-are-your-web-browser/
62 http://blog.intego.com/2010/06/10/att-data-breach-affects-ipad-users/
63 http://blog.intego.com/2010/08/03/web-attack-pinpoints-where-you-live/
64 http://blog.intego.com/2010/10/01/95-of-all-e-mail-is-spam-2/
65 http://blog.intego.com/2010/12/31/spam-is-down-but-theres-still-plenty-to-go-around/
66 http://blog.intego.com/2010/10/26/are-any-passwords-secure-any-more/
67 http://blog.intego.com/2010/12/14/passwords-in-the-news-are-yours-secure/