The Year in Mac Security 2009

An Annual Report from Intego

2009 was another busy year for Mac security and malware, with new threats targeting Macs, iPhones being attacked, and a large number of Mac OS X vulnerabilities. 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

The year in malware began in January 2009, shortly after Apple announced new software at the Macworld Expo in San Francisco. The company's iWork '09 suite of productivity software was updated in January, and no sooner had it been released than malware writers took advantage of it. The iServices Trojan Horse[1] was provided as an additional installation package inside an installer for iWork found on BitTorrent trackers and other sites containing links to pirated software.

This was all the more interesting as the iWork disk image was more than 450 MB; hardly something that one would download casually. Yet it was effective; in just a short time, Intego found that more than 20,000 people had downloaded the infected disk image. The iServices Trojan opened a backdoor on infected Macs, and it connected to remote servers to download new code. It was actively used as part of a botnet that was involved in distributed denial of service attacks and more.

Shortly thereafter, given the success of the first version of the iServices Trojan, the same cyber-criminals planted the next version of their malware with copies of Adobe Photoshop CS4 for Mac found on BitTorrent trackers[2]. The actual Photoshop installer was clean, but the Trojan horse was found in a crack application used to serialize the software. Functioning in a similar manner as the first version, the iServices.B Trojan horse allowed remote users to perform actions on infected Macs.

The RSPlug Trojan horse, which Intego first discovered in October 2007, was as virulent as ever. Variants to the RSPlug were found throughout the year, often masquerading as a video codec, including one in February[3], two in June[4] [5], and two in July[6] [7].

One of the new variants, in March[8] 2009, was written especially to taunt Intego. In December 2008, one variant had already done this, containing code which said "begin 666 intego." This tells the system to create a file with read and write 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 malicious code, named "intego". The new version contained the following code:

```
niagasekirtsogetni 666 nigeb
```

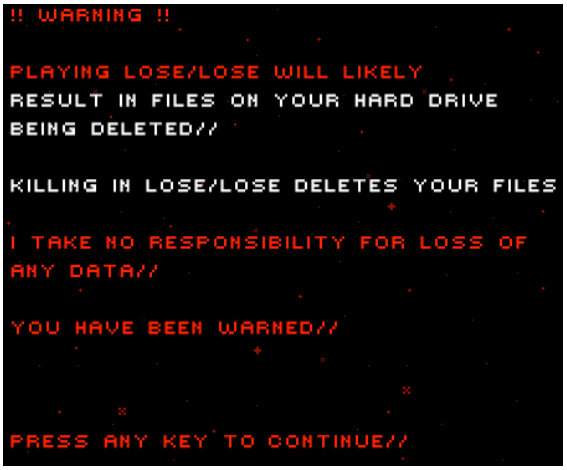
This line of code, when held up to a mirror, says "begin 666 IntegoStrikesAgain". Needless to say, Intego VirusBarrier's proactive detection spotted this new variant, and all others, right away, and Intego

updated its VirusBarrier definitions immediately. Users who were protected from malware by VirusBarrier were never at risk from these variants.

In April, Intego discovered a proof-of-concept malware called Tored.A[9], an application created with RealBasic, a version of the BASIC programming language available for Mac OS X, Windows and Linux. The malware in question was a self-contained application containing RealBasic code and a runtime needed for that code to execute. The malware attempted to copy itself to the System folder and the System/Library/StartupItems folder, renaming itself "applesystem" or "systemupdate". It obtained e-mail addresses from Address Book, and sent e-mails to recent recipients containing a copy of the malware, but did so with an SMTP server that was non-existent at the time. This malware also attempted to create a botnet, recorded some keystrokes, and attempted to copy itself to other disks that were mounted.

While this malware was not found in the wild, Intego considered the use of RealBasic and its runtime to be a novel approach to malware. Because of this, Intego created a new malware class for VirusBarrier. However, the code in this malware was faulty, and it did not work correctly, so there was no real threat from this malware.[10]

In October, a game was released that deleted files on users' Macs when they played it. This game, called lose/lose[11], was designed to do this. As the creator said, "Each alien in the game is created based on a random file on the player's computer. If the player kills the alien, the file it is based on is deleted. If the player's ship is destroyed, the application itself is deleted." That there was a warning was all well and good, but the game did delete users' files, so it was treated as malware.



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. In February, IBM issued its X-Force 2008 Trend and Risk Report[12] which showed that Apple was at the head of the league table for security vulnerabilities. Apple issued a total of 34 security updates in 2009 for Mac OS X, Apple software and Apple hardware.

Throughout the year, Apple issued security updates for specific software. A flaw in the way Safari handled RSS feeds was found in January[13], 50 security flaws for Safari were patched in June[14], two more in July[15], another six in August[16], and more in November[17]; a PDF vulnerability initially found to affect Adobe Acrobat was found to also affect Apple's Preview in February[18]; an iTunes security issue was patched in March[19] and another in September[20]; a QuickTime flaw was patched in June[21], and four QuickTime bugs were fixed in September[22], shortly after the release of Snow Leopard; a security update was released for GarageBand in August[23]; Apple issued a special security update for the BIND DNS server in August[24]; and Apple sent out a security update for its Xsan file system in September[25].

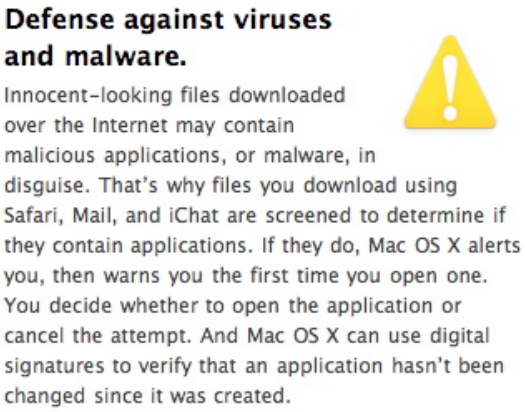
Unfortunately, some of these updates were long in coming. In May[26], a security researcher questioned why Apple had not patched a known Java vulnerability for more than six months. He showed how easy this vulnerability was to exploit, by creating a proof-of-concept Java applet on his web site. (Apple finally updated Java to fix this and some 150 other bugs in June[27].)

In April, a kernel vulnerability was found[28] with potentially serious consequences. Unlike current Trojan horses, which require that a user enter an administrator's user name and password, an exploit was made public that could grant root access to malicious software with no password required. It took advantage of a vulnerability that existed when volumes (hard disks, disk images, removable media or network volumes) are mounted in Mac OS X. When this occurred, root access could be obtained without needing a password. The volume itself needed to be

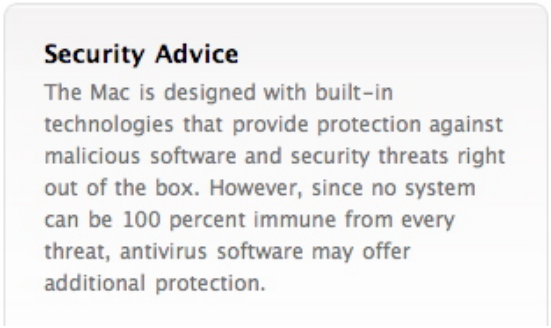
"prepared" for this exploit to work, but such a malicious program could simply create a disk image when it launched, mount the disk image, allowing the exploit to function, then unmount it. The danger of such an exploit was obvious: since no password is required, users get no warning. A malicious program could be disguised as a graphic file, music file or PDF, or a simple application.

In May[29], Apple released the largest security update yet for Mac OS X, with 47 security fixes in an update that was more than 400 MB.

In June, just a few months before the release of Mac OS X 10.6, Snow Leopard, Apple recognized the threat of malware to Macs on a page dedicated to security for Snow Leopard. On Apple's web page outlining security features in Snow Leopard, the company discusses features that provide "Defense against viruses and malware," such as warnings when users open applications they have downloaded, a feature that has existed since Mac OS X 10.4. This page also states that "Mac OS X offers a multilayered system of defenses against viruses and other dangerous malware," such as "sandboxing," a method of restricting the actions that applications have to an operating system or its files, library randomization, which "prevents malicious commands from finding their targets," and execute disable, which protects memory from attacks.



Beyond recognizing the malware threat to Macs, Apple went further, admitting that the techniques it includes in Mac OS X aren't enough to fully protect Macs from viruses and malware. The company provided security advice, as Intego has said for many years, saying, "since no system can be 100 percent immune from every threat, antivirus software may offer additional protection."



Apple had always suggested, especially in its TV commercials, that malware targeting the Mac did not exist. This change in the company's position shows that Apple has realized that the threat was real.

So when we got reports in late August that Snow Leopard was to contain an antivirus[30], we weren't totally surprised. What was surprising, however, was the limited scope and effectiveness of this built-in anti-malware feature[31]. It turned out that this feature only scanned files downloaded with a handful of applications, only when those files were double-clicked or opened, and only scanned for two Trojan horses. In fact, as of January 2010, this anti-malware feature has not been updated, and still scans for the same two Trojan horses and nothing else. In September, following the release of Snow Leopard, Intego published detailed information[32] about how this feature works.

In August[33], just before the release of Mac OS X 10.6, Snow Leopard, Apple released an update for Mac OS X 10.5 which contained a number of security fixes.

After Snow Leopard was released, it was found that it shipped with an insecure version of Flash Player[34], which wasn't updated until the first general update for Mac OS X 10.6.

In September, just after the release of Snow Leopard, Apple released a security update for Java for Mac OS X 10.5[35]. This very large (161 MB) update patched 25 bugs in Java. This was followed by a bug-fix update for Snow Leopard in September[36], which contained a number of security fixes, notably one to bring Flash Player up to date. At the same time, Apple released another security update for Leopard[37], Mac OS X 10.5, patching 33 bugs.

A serious bug in the way Snow Leopard handled the Guest user account was found in September[38]. A number of Mac users found that their home folders disappeared after logging in on their Macs with the Guest account. (The Guest account is a special account, activated in the Accounts preferences, whereby a user

can log in with no password, and, at log-out, all their data is deleted. It's great for one-time logins.) This happened to people who turned on the Guest account option under Leopard; there was something wrong with the way Snow Leopard transferred this setting to the new version of the OS. Apple fixed this in its November security update to Snow Leopard.

In November, that update[39] contained dozens of security fixes, and weighed in at 157 MB to 473 MB. Not only did it fix the Guest account issue, but it fixed an odd flaw whereby "A design issue in Dictionary allows maliciously crafted Javascript to write arbitrary data to arbitrary locations on the user's filesystem."

December saw an update to Java[40], for both Leopard and Snow Leopard, fixing more than two dozen bugs.

iPhone Security Issues

2009 was a busy year for security researchers who focus on the iPhone. In June, Apple released the iPhone OS 3.0, which contained more than 40 security fixes[41].

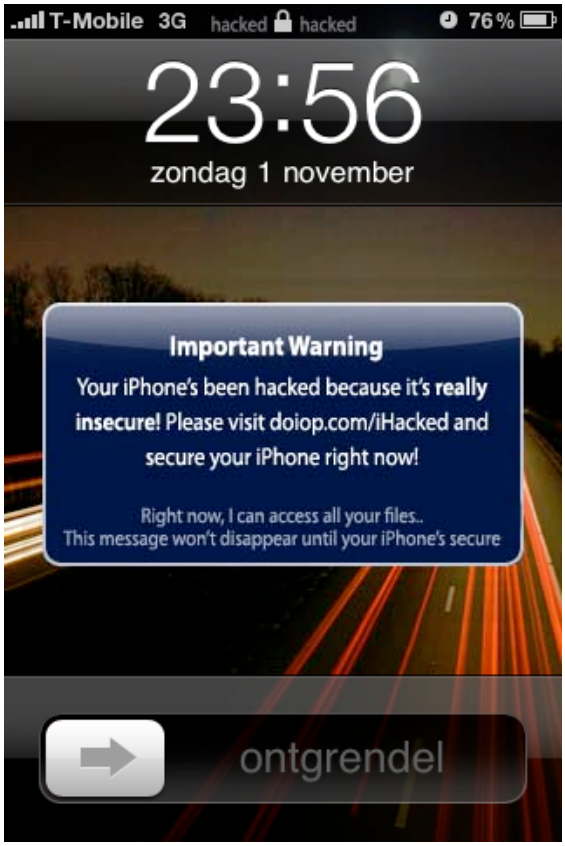
In July[42], security researcher Charlie Miller found a vulnerability in the way the iPhone handles text messages (SMSs), which could allow remote, malicious users to monitor where an iPhone was, using its built-in GPS, use its microphone to record conversations, or use it as part of a botnet. Apple patched this vulnerability in August[43].

Jailbroken iPhones were in the news in 2009. Jailbreaking is when a user removes Apple's barriers to installing third-party applications, allowing users to install software that is not distributed via the iTunes Store, as well as cracked software. It also allows users to use the iPhone with carriers other than the exclusive carrier in their country. (iPhones without carrier limitations are sold in a handful of countries, but currently not in the US.)

A number of issues and malware plagued such iPhones. In July[44], Charlie Miller pointed out that jailbreaking removes about 80 percent of the security protections built into the iPhone software, leaving users open to a wide variety of attacks. In late July[45], Apple published a support document discussing the risks and dangers inherent in jailbreaking an iPhone, but this didn't stop a lot of people from taking these risks.

Apple updated the iPhone OS to version 3.1 in September[46], including ten security fixes in this update. This update also contained a new security feature that Apple didn't talk about: anti-phishing protection for the iPhone[47]. When this was first discovered, it didn't work correctly, but it was later found that users needed to perform certain operations to get the feature to work[48].

The iPhone was at the forefront again in November, when a Dutch hacker came up with a novel way to make a few euros[49]. Realizing that jailbroken iPhones are generally accessible via ssh, he "broke into" them, then sent SMS alerts to their owners, telling them the phones were insecure. For 5 euros, he'd be happy to tell them how to secure their phones.



This highlighted the fact that most iPhone users who jailbroke their phones, and who installed OpenSSH, did not change the default passwords. The hacker simply used port scanning to find vulnerable iPhones and sent the warning to them.

This flaw in jailbroken phones would be in the news for a while. Later in November, an Australian hacker decided to try his hand at an iPhone worm[50]. This worm, called the ikee worm, initially meant as a

"prank", installed an image of Rick Astley as wallpaper, then turned off ssh (thereby making the "infected" phone safer), before sniffing around to try and find other phones to infect. Created by an unemployed Australian programmer, this "prank" seemed to have gotten a bit out of control. While it can't infect all jailbroken iPhones—some phone networks use NAT (network address translation) that prevents direct access to an iPhone using an IP address, and others block ssh packets on their networks—the worm spread outside its native Australia.

Later in November, Intego discovered a hacker tool that was able to copy personal information from jailbroken iPhones[51]. This hacker tool, iPhone/Privacy.A, takes advantage of the same vulnerability in the iPhone as the ikee worm, allowing hackers to connect to any jailbroken iPhone or iPod touch whose owners have not changed the root password.

When connecting to a jailbroken iPhone, this tool allows a hacker to silently copy a treasure trove of user data from a compromised iPhone: e-mail, contacts, SMSs, calendars, photos, music files, videos, as well as any data recorded by any iPhone app. Unlike the ikee worm, which signals its presence by changing the iPhone's wallpaper, this hacker tool gives no indication that it has invaded an iPhone, and leaves no traces.

Hackers using this tool, written in Python, could install it on a computer—Mac, Windows, Unix or Linux—then let it work. It scans the network accessible to it, and when it finds a jailbroken iPhone, breaks into it, then steals data and records it.

This hacker tool could easily be installed, for example, on a computer on display in a retail store, which could then scan all iPhones that pass within the reach of its network. Or, a hacker could sit in an Internet café and let his computer scan all iPhones that come within the range of the wifi network in search of data. Hackers could even install this tool on their own iPhones, or other smartphones, and use it to scan for jailbroken phones as they go about their daily business.

Later in November, Intego discovered another iPhone worm, iPhone/iBotnet.A[52], which was capable of spreading across a network, and also hijacking jailbroken iPhones or iPod touches for use in a botnet.

This worm, which was created based on the code of the ikee worm, starts by searching its local network, as well as a number of IP address ranges, for available devices to infect. The address ranges it scans include those of ISPs in the Netherlands, Portugal, Hungary, Australia, and if an appropriately unprotected iPhone is found, the worm can copy itself to these devices.

When active on an iPhone, the iBotnet worm changes the root password for the device (from "alpine" to "ohshit"), in order to prevent users from later changing that password themselves. It then connects to a server in Lithuania, from which it downloads new files and data, and to which it sends data recovered from the infected iPhone. The worm sends both network information about the iPhone and SMSs to the remote server. It is capable of downloading data, including executables that it uses to run and carry out its actions, as well as new files, providing botnet capabilities to infected devices. (A botnet is a network of infected computers or devices that can be controlled by hackers to attack other computers, serve malware, send spam, serve pages or images, and much more.)

The worm also gives each infected iPhone a unique identifier; this to be able to reconnect easily to any iPhones on which valuable information is found, but also to ensure that only infected iPhones can connect to the server. Finally, it adds a new entry for the IP address of a Dutch bank web site to the iPhone's /etc/hosts file, to lead Dutch users who connect to this bank site to a bogus site, presumably to harvest user names and passwords.

Third-Party Software and Macs

Third-party software—that from vendors other than Apple—was the cause of much worry in 2009. 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 11 times for security fixes. Adobe software—especially Flash Player and Acrobat—required frequent updates, with two updates for Flash Player and four for Acrobat. And Microsoft Office was updated three times for security fixes.

A zero-day flaw in Acrobat and Adobe Reader, discovered in December[53], did not seem serious at first, but may have been used, in part, in a massive hacking attack on a number of US companies. Adobe didn't patch this flaw until mid-January 2010.

But the security fixes required went further than the usual software. In a rare hardware issue, a number of Hewlett-Packard printers were found to have "A potential security vulnerability . . . [that] could be exploited remotely to gain unauthorized access to files."[54]

Other Security Issues

Phishing—attempts to trick users into entering personal information, such as user names, passwords and credit card numbers, on web sites that look legitimate—has been a serious issue for years. Phishers often target users of banks or major e-commerce web sites. In February, we saw well-composed phishing e-mails that targeted users of Apple's MobileMe service[55], showing that Mac users are a valid group of people to target for this type of scam.

Hacking contests were held during the year, notably one in which security researcher Charlie Miller hacked a Mac in 10 seconds[56]. To be fair, he didn't discover a way to hack a Mac in 10 seconds, but had worked for weeks to find out how to exploit a flaw in the Safari web browser. When the contest started, he knew exactly what to do to have the test Mac hacked.

Conclusion

2009 was a very busy year for Mac security professionals. Not only did Trojan horse threats increase during the year, with a number of new variants, and new web sites serving this malware, but many operating system and third-party software vulnerabilities were found that compromised the security of Macs.

Many of these operating system vulnerabilities pave the way for unseen malware attacks. Some of them are such that merely visiting a booby-trapped web page can compromise a Mac. This underscores the importance of security software that protects not only from malware but also from web threats and the many other kinds of menaces that target Macs. It also highlights the need to keep software up-to-date. Both for Mac OS X and for third-party software, users should make sure that they have the latest versions of their software, since some programs—such as Adobe Reader, commonly used to view PDF files—are easy to attack with known exploits circulating in the wild.

The past year also saw a rise in attacks on the iPhone. This is not surprising, given the success of the device, but it is important to note that these attacks have so far only affected jailbroken iPhones. Users should think carefully if they want to take the risk of removing Apple's protection on their iPhones before jailbreaking them.

1 http://blog.intego.com/2009/01/22/mac-trojan-horse-osxtrojaniservicesa-found-in-pirated-apple-iwork-09/
2 http://blog.intego.com/2009/01/26/new-variant-of-mac-trojan-horse-iservices-found-in-pirated-adobe-photoshop-cs4/
3 http://blog.intego.com/2009/03/17/new-rsplug-trojan-horse-variant-new-code-new-theater-of-operations/
4 http://blog.intego.com/2009/06/19/new-rsplug-trojan-horse-variant-found-on-game-sites/
5 http://blog.intego.com/2009/06/26/new-variant-of-rsplug-trojan-horse-rsplug-l/
6 http://blog.intego.com/2009/07/02/new-variant-of-the-rsplug-trojan-horse/
7 http://blog.intego.com/2009/07/21/new-version-of-rsplug-trojan-horse-masquerading-as-mac-os-x-crackkeygen/
8 http://blog.intego.com/2009/03/12/new-variant-of-rsplug-trojan-hackers-taunt-intego-again/
9 http://blog.intego.com/2009/04/29/intego-discovers-a-new-proof-of-concept-malware/
10 http://blog.intego.com/2009/04/29/intego-discovers-a-new-proof-of-concept-malware/
11 http://blog.intego.com/2009/10/29/loselose-is-it-a-game-is-it-malware-its-both/
12 http://blog.intego.com/2009/02/12/apple-stays-at-the-top-of-operating-system-vulnerability-league-table/
13 http://blog.intego.com/2009/01/13/critical-safari-rss-vulnerability-and-how-to-fix-it/
14 http://blog.intego.com/2009/06/09/apple-releases-dozens-of-security-fixes-for-safari-4/
15 http://blog.intego.com/2009/07/09/apple-updates-safari-with-security-fixes/
16 http://blog.intego.com/2009/08/12/apple-plugs-six-holes-in-safari-update/
17 http://blog.intego.com/2009/11/12/apple-updates-safari-includes-security-fixes/
18 http://blog.intego.com/2009/02/24/acrobat-vulnerability-present-in-apples-preview/
19 http://blog.intego.com/2009/03/12/itunes-81-ships-with-security-fix/
20 http://blog.intego.com/2009/09/23/apple-updates-itunes-fixes-a-security-hole/
21 http://blog.intego.com/2009/06/02/apple-updates-itunes-and-quicktime-security-fixes-included/
22 http://blog.intego.com/2009/09/10/apple-issues-quicktime-security-update-for-tiger-and-leopard/
23 http://blog.intego.com/2009/08/04/apple-issues-security-update-for-garage-band/
24 http://blog.intego.com/2009/08/12/apple-issues-security-update-for-bind-dns-server/
25 http://blog.intego.com/2009/09/15/apple-issues-security-update-for-xsan-file-system/
26 http://blog.intego.com/2009/05/20/apple-hasnt-updated-java-to-protect-mac-users-from-critical-vulnerabilities/
27 http://blog.intego.com/2009/06/16/apple-finally-updates-java-after-six-months/
28 http://blog.intego.com/2009/04/17/mac-os-x-kernel-vulnerability-could-lead-to-dangerous-malware/
29 http://blog.intego.com/2009/05/13/apples-patch-tuesday-mammoth-security-updates/
30 http://blog.intego.com/2009/08/25/snow-leopard-contains-an-antivirus/
31 http://blog.intego.com/2009/08/28/intego-virusbarrier-x5-compared-to-apples-mac-os-x-10-6-snow-leopard-anti-malware-function/
32 http://blog.intego.com/2009/09/02/how-the-anti-malware-function-in-apples-snow-leopard-works/
33 http://blog.intego.com/2009/08/06/apple-updates-mac-os-x-includes-security-fixes/
34 http://blog.intego.com/2009/08/31/snow-leopard-ships-with-insecure-version-of-flash-player/
35 http://blog.intego.com/2009/09/04/apple-releases-java-security-update-for-10-5/
36 http://blog.intego.com/2009/09/11/apple-updates-snow-leopard-includes-security-fixes/
37 http://blog.intego.com/2009/09/11/apple-releases-large-security-update-for-leopard/
38 http://blog.intego.com/2009/09/22/1155/
39 http://blog.intego.com/2009/11/10/apple-release-os-x-update-with-dozens-of-security-fixes/
40 http://blog.intego.com/2009/12/04/apple-issues-updates-for-java-in-leopard-and-snow-leopard/
41 http://blog.intego.com/2009/06/18/iphone-os-3-0-includes-more-than-40-security-fixes/
42 http://blog.intego.com/2009/07/02/apple-scrambling-to-patch-sms-flaw-in-iphone/
43 http://blog.intego.com/2009/08/01/apple-updates-iphone-for-sms-vulnerability/
44 http://blog.intego.com/2009/07/02/jailbroken-iphones-are-weak-on-security/
45 http://blog.intego.com/2009/07/30/apple-highlights-risks-of-jailbreaking-iphones/
46 http://blog.intego.com/2009/09/10/iphone-and-ipod-touch-updates-contain-security-fixes/
47 http://blog.intego.com/2009/09/10/apple-adds-safari-anti-phishing-feature-that-doesnt-work-to-iphone/
48 http://blog.intego.com/2009/09/14/response-from-apple-regarding-iphone-anti-phishing-problem/
49 http://blog.intego.com/2009/11/03/iphone-ransomware-dutch-hacker-exploits-jailbroken-iphone-bug-and-asks-for-money/
50 http://blog.intego.com/2009/11/09/worm-affects-jailbroken-iphones-changes-wallpaper/
51 http://blog.intego.com/2009/11/11/intego-security-memo-hacker-tool-copies-personal-info-from-iphones/
52 http://blog.intego.com/2009/11/23/intego-security-memo-iphone-worm-creates-botnet-copies-personal-data/
53 http://blog.intego.com/2009/12/15/zero-day-adobe-acrobat-and-reader-attacks-in-the-wild/
54 http://blog.intego.com/2009/02/09/hp-printers-open-to-unauthorized-access-security-fix-available/
55 http://blog.intego.com/2009/02/12/mobileme-users-beware-phishers-are-targeting-you/
56 http://blog.intego.com/2009/03/19/hacker-contest-mac-hacked-in-10-seconds/