White Paper

McAfee®

Downloading from Mobile App Stores Is a Risky Business

By Anthony Bettini and Michael Price

McAfee® Labs™

Table of Contents

In the past few years, vulnerabilities in network services have become increasingly difficult to find in widely deployed server software. Attackers have also found more effective ways to make money from hosts compromised using client-side vulnerabilities. This improvement in security and in the ability for attackers to make money has led to a shift in focus from network-based to client-side vulnerability research. Researchers now find more vulnerabilities in popular client applications such as Microsoft Office, web browsers, Adobe Flash, and Adobe Reader, while seeing fewer in traditional targets such as Apache HTTP Server, OpenSSH, and Microsoft RPC. This shift has paralleled the growth in malware exploiting client-side vulnerabilities on compromised websites or coupled with spam. With the ever-expanding prevalence and growing importance of mobile applications, a further shift in focus to mobile application security—particularly client-side vulnerabilities in apps such as Mobile Safari—is both predictable and underway.

Introduction

Sandboxing, an approach used to isolate apps and content from vital system components and other applications, has improved security, particularly in the case of Google Chrome, Adobe Reader X, and mobile devices. Chrome implemented a sandbox to protect the browser, Reader X to encapsulate PDF viewing, and mobile devices to protect apps from interfering with the security of the phone's underlying operating system and other applications running on the device. However, sandboxing is not a panacea. For example, the malware proof-of-concept OSX/iPHSponey.A[1] was able to collect substantial personal data while working entirely within the iOS sandbox. In addition to evolving client-side attacks against sandboxed applications, iOS jailbreaking (removing limitations on an Apple device) has led security researchers to pay close attention to sandbox exploits. Comex's JailBreakMe.com iOS sandbox escape attack[2] and the "rageagainstthecage"[3] Android sandbox escape attack are two high-profile examples. Further, with refinements in new, sophisticated exploitation techniques (such as return-oriented exploitation [ROP]), attacking embedded systems and mobile devices has become more practical.

"Attacks" Beyond Malware and Vulnerabilities

Before examining technical attacks, let's first take a look at "review fraud" issues within some app store rating models. We can better understand these issues by comparing them with other review rating systems, such as Google's PageRank search-engine ranking system. PageRank fraud occurs when an attacker poisons search results to make his or her site appear disproportionately high in search results. Instead of an attacker's site appearing in a realistic position within search results, the site is listed higher than far more popular sites. A similar fraud appears to be taking place in some app store communities. For instance, the ordering of app store search results, the equivalent of PageRank for an app store, is based largely on reviews and ratings. More reviews and more ratings result in higher ordering for an app in a user's search results. Just as PageRank fraud brings more clicks to malware sites, app store rating fraud results in more users clicking on an app to purchase it. Apple's App Store doesn't require a reviewer to have purchased an app to rate it; thus, it is easy for an "attacker" (typically an app author or app affiliate) to increase the ranking of an app by submitting reviews. Further, as these are generally fake reviews, the "star rating" is typically much higher than the average review, and the comments are usually much more positive. This has the added effect of increasing the likelihood of a consumer's being duped into paying for the app.

[1] http://vil.nai.com/vil/content/v_246873.htm
[2] https://github.com/comex
[3] http://intrepidusgroup.com/insight/2010/09/android-root-source-code-looking-at-the-c-skills/

How can Apple and other app store vendors wrestle this problem to the ground? Isn't it unsolvable?

Yes and no. Fake reviews are likely an inherent risk in any review-based system. However, similar to how Amazon developed and refined its review system over time, Apple and others will need to take similar steps. The first is likely inevitable: reviews and star rankings must be restricted to users who have both paid for and downloaded that version of the app. Currently, Apple appears to have prioritized usability over reliability of rankings in this case. However, as attacks increase and user satisfaction decreases, this prioritization is likely to change.

Attackers could fight back by creating one-time email addresses, purchasing the app, and then writing a review. But Apple could take the next step by validating IP uniqueness, referring URLs, browser/system metadata, and other properties. These approaches have their pros and cons. The point remains, however, that the current system doesn't do enough and is likely to be improved.

Distributed Challenges—the Android Market

Other app stores, such as the Android Market, have an altogether different model. In the case of Android apps, most phones allow the "side-loading" of apps and are not restricted to getting them from a centralized app store, as they must with Apple. This openness means that Android app developers, or others, could post Android apps on their websites and attempt to attract users to install them. The situation sounds a lot like the drive-by download malware model. Unlike Apple's situation, there is no central place where Google can check all apps for suspicious behavior (other than on the phone itself).

In the case of the widely publicized Geinimi,[4] found on Android devices in China, the malware bound itself to popular apps to steal personal information from devices. This type of attack would be difficult for Google to detect if the apps were distributed on the Internet outside of the Android Market, as Google's ability to secure the device is limited to on-device scanning. Apple, on the other hand, analyzes apps when they are submitted to the store (with one notable exception we discuss below).

Security-conscious users in the United States have also discovered malware-infected apps.[5] Recently, the researcher Lompolo found a series of Android applications carrying backdoor Trojans in the Android Market and actively being downloaded.[6] The applications were discovered because Lompolo noticed that some of the Android apps in question appeared to have been republished by the wrong publisher—in other words, that they had been pirated and then repackaged. This is not the usual case of piracy, in which someone attempts to use software without paying for it. In this case, the malware author repackaged software from another publisher, presumably without permission or distribution rights. While reverse engineering one of the pirated apps, Lompolo noticed the app used the "rageagainstthecage" Android sandbox escape exploit, as well as stored information in a local SQLite database, communicated with a suspect web server by IP address, and posted the device's IMEI and IMSI codes (which could identify the device) to the remote server. Google was quick to remove offending applications from the Android Market[7] and has also since released a tool to help affected users recover from the effects of this attack.[8] However, with estimated downloads in the tens of thousands to the hundreds of thousands, the number of users who could be affected remains significant. It's likely this event will cause Google to revisit its position of allowing applications to be posted to the Android Market in such an unrestricted fashion.

[4] http://vil.nai.com/vil/content/v_342726.htm

[5] http://venturebeat.com/2011/03/02/dozens-of-android-apps-pulled-from-market-due-to-malware-infections/?source=business-insider

[6] http://www.reddit.com/r/netsec/comments/fvhdw

[7] http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/

[8] http://googlemobile.blogspot.com/2011/03/update-on-android-market-security.html

What Do BitTorrent and Apptrackr Have in Common?

To answer this question let's first review a bit of the history of computer piracy. For obvious reasons, discussions of piracy (other than its ill effects) are rarely documented. However, just as blocking crimeware requires knowledge of how crimeware systems work and how criminals profit, monitoring other malware distribution channels typically requires knowledge of those systems as well. To shed light on how pirated apps for mobile devices are likely to contain more malware over time, we'll take a look at how the evolution of pirated PC software led to more bundled malware.

Pirated software in the PC world evolved from people trading software on hard media like floppies, to distributing software on bulletin board systems (which were themselves distributed in nature), to trading on the Internet via closed systems such as FTP, to trading on the Internet via open systems like IRC and newsgroups, to eventually trading on fully public and unrestricted systems like BitTorrent. All of these methods are still used today, but the key is that these pirated software systems became more easily accessible and open over time. With the majority of peer-to-peer (P2P) traffic, on a per country basis, becoming more specific to one P2P app (such as BitTorrent in the United States), malware on BitTorrent has exploded. A few years back, we wouldn't have imagined a reputation system for pirated software; just the idea of it would have been ludicrous. Now certain BitTorrent tracker sites allow users to mark software as infected, bad, or other designations.

Apptrackr takes the place of BitTorrent for mobile apps. Like BitTorrent tracker sites, not every Apptrackr link connects to a pirated app. But also like the BitTorrent tracker sites, most of the resulting Apptrackr traffic is likely from pirated app downloads.

Why does this matter in a discussion of app store download safety? When you click on "App Store" on an Apple iOS device, you enter Apple's store. On a jailbroken phone that is reconfigured for installing pirated apps, the Installous app acts like Apple's App Store, but points to Apptrackr to get the pirated apps. Installous itself is an app store, albeit one that uses Apptrackr as a proxy to obtain the apps, which are further proxied through file-hosting sites.

From an analysis perspective, however, just as BitTorrent made obtaining pirated software much easier for consumers—resulting in more malware-infected links on BitTorrent—Apptrackr has made downloading pirated iOS applications much easier for consumers.

Can you see where this is going? Apptrackr, over time, will link to more malware-infected iOS applications (mostly of pirated apps). Now interestingly enough, most malware is small in nature. If you look at malware sizes for drive-by downloads, the average is something much smaller than one megabyte. This is because the malware tries to hide the fact that a download is occurring by minimizing its file size. However, in the case of pirated software, the opposite is true. Users know they are downloading software, so there is nothing to hide. Thus, it would be far easier to hide a Trojan or other malware in a large app than a small one (like a needle in a haystack). In the case of Apptrackr, all of the pirated apps have been cracked. So even if there were a public database of hashes to validate unmodified apps (which there isn't), in the case of pirated apps, this would fail because the apps have been cracked and are inherently modified. This makes finding a Trojan or backdoor malware all the more difficult.

Late last year, we did a quick check of some of the largest apps (in file size) on Apptrackr, and were able to find an app link that pointed directly to malware (an EXE). In this case, it wasn't a backdoor, nor would it even run on the phone. It was targeted at users of Apptrackr's portal; they used Microsoft Windows-based hosts to download apps and then copy them manually into Apple iTunes. This app has since been replaced, and the tracking link no longer points to malware, but here we see the tip of the iceberg. Just as BitTorrent is currently flooded with malware that appears to be pirated apps and the latest Hollywood movies, so too will Apptrackr likely become increasingly infected with malware. In the case of BitTorrent, client-side anti-malware solutions offer some defense; in the case of mobile devices such as phones, however, most lack similar protection.

"Targeted" Attacks

Recently, students in Germany figured out how to perform a key-recovery attack against a jailbroken iPhone.[9] Further, they jailbroke the iPhone even when it was locked by Apple password protection.[10] If attackers in the wild were to do this, they likely could combine this technique with other known remote exploitation techniques for iOS to recover the credentials to financial or shopping cart applications, either of which could profit the attackers. Furthermore, in the case of credit card transaction-processing applications, such as Square or its competitors, the attacker who compromised the phone could perhaps install a backdoor that monitors the use of the credit card validation process and forwards the credit card information at a later time. A proof of concept somewhat similar to this was demonstrated recently at ToorCon.[11] Although this type of attack probably hasn't yet occurred in the wild, as mobile phones become increasingly entrenched in our lives—particularly in the area of commerce and transactions—such attacks will become more likely.

Another recent development has arisen in determining installed applications. A privacy hole in iOS could allow a person to determine which music or apps another user of iTunes has purchased.[12] Although this "attack" is a low risk for several reasons, it is relevant for an attacker to know which applications are installed on a given device targeted for attack. We expect an increase in the near term in information gathering and privacy attacks against mobile devices.

Likely Evolutions for App Stores

Growth in the number of mobile apps in app stores has exploded. The sheer volume of apps has, in some cases, made it hard for users to separate the apps they are interested in from those they are not interested in. Features such as Apple's Genius recommendations, a reputation-based recommendation system for mobile apps, are likely to become increasingly important and greatly enhanced. For centralized app stores such as Apple's, vendors are likely to spend more and more resources on back-end automation to check the behavior and application programming interface (API) calls of applications for safety and security reasons. Some companies that offer application security analysis services have recently offered support for iOS and Android applications, further promoting this theory. Further, ratings, recommendations, download counts, and sales metadata are all likely to become more centralized and tracked for validity (to feed application reputation systems). Especially given the high-profile nature of the recent series of apps with backdoor Trojans in the Android Market, it is likely that Google will introduce either some level of federation or of automated security scanning of newly posted apps.

Exercise Caution

In the face of risk, both enterprises and consumers need to exercise caution. The familiar rules apply: download only software and visit only URLs that are, in at least some sense, trusted. Enterprises should consider a policy of blocking all jailbroken iOS devices from accessing the corporate network (including email) because these devices have a greater chance of having untrusted software installed on them. For consumers, using pirated apps is both illegal and unsafe. Imagine running a cracked app on the same device that multitasks with banking apps—certainly not a good idea. With even "legitimate" apps suspect, as in the case of the recent Android Market apps carrying backdoor Trojans, both consumers and enterprises must protect themselves.

[9] http://www.sit.fraunhofer.de/en/Images/sc_iPhone%20Passwords_tcm502-80443.pdf
[10] http://www.youtube.com/watch?feature=player_embedded&v=uVGiNAs-QbY
[11] http://sandiego.toorcon.org/index.php?option=com_content&task=view&id=48&Itemid=9
[12] http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation

About the Authors

Anthony Bettini is part of the McAfee Labs senior management team. Prior to McAfee, he worked at McAfee Foundstone®, Guardent, Bindview, and as an independent security contractor. Bettini specializes in software security and vulnerability detection and has spoken publicly for NIST, the Computer Anti-Virus Research Organization (CARO) in Europe, RSA Europe, and at the twenty-second Annual FIRST Conference in Miami on location-specific threats. Bettini has published new vulnerabilities found in Microsoft Windows, ISS Scanner, PGP, Symantec ESM, and other popular applications. In addition to contributing to a handful of security books, he was the technical editor for *Hacking Exposed, 5th Edition* (McGraw-Hill/Osborne).

Michael Price, senior operations manager for McAfee Labs in Latin America, is responsible for the day-to-day operations of the McAfee Labs office in Chile. In this role, he leads a cross-functional team of researchers that produces industry-best content for cloud, anti-virus, threat intelligence, quality assurance, and vulnerability content streams. Previously, Price was the research manager for McAfee Foundstone Enterprise. In this role, he worked with and managed a global team of security researchers responsible for implementing software checks designed to detect the presence of vulnerabilities on remote computer systems. Price has extensive experience in the information security field, having worked in vulnerability analysis and software development for nearly 11 years.

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence™.[13] The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.
http://www.mcafee.com

[13] http://www.mcafee.com/us/mcafee-labs/technology/global-threat-intelligence-technology.aspx

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee, the McAfee logo, McAfee Labs, McAfee Global Threat Intelligence, and McAfee Foundstone are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied.