APP SOLID.

Powerful mobile app security solution

iOS Backloading and Rogue App Stores : A Major Threat to iOS Developers

---

Contributors – Kayla Bayens, Mary Min

Research Paper : Mobile Security

iOS Backloading and Rogue App Stores : A Major Threat to iOS Developers

---

Contents

Introduction

One main concern for a mobile application developer or publisher is having their app hacked or reverse engineered, which can lead to a multitude of problems including piracy, leaked user data, and malware infested fake versions. The most common path to reverse engineering a mobile application is through decompiling the app and obtaining the source code for analysis and replication. According to Scott Milliken, CEO of MixRank, a monitoring and early detection company, “Software engineers that are accustomed to writing web applications - where the hardware is secured and trusted - have migrated en mass to writing mobile apps, carrying along the same security mindset. This has resulted in a hacker’s treasure trove of exposed keys and sensitive IP leaks. Adversaries and some security professionals have noticed, but app developers are always shocked to learn what they’ve accidentally published.” There is simply not enough time to do a full security audit before every version release, and security blunders are made by the thousands in new app releases every day, largely going unnoticed by the developer. Although Google and Apple have review processes in place, official app stores aren’t safe from pirated apps - with millions of published apps and thousands new apps published every day, it’s impossible to review all of them before they are published to billions of users with your code, functionality and even branding. And the problem is even more serious in unsanctioned, unofficial, pirated app stores. In the past it was believed that this fear was regulated primarily to the Android platform because of its open source nature which allowed for multiple marketplaces and no-review, instant market submission process. iOS on the other hand was considered safer because there was only one App Store, the apps underwent a lengthy review process, and required jailbreaking of the phone. Jailbreaking a phone was complicated and each subsequent iOS update would render the phone useless, making the rewards of unsanctioned iOS app stores not worth the effort to the average consumer. However, over the last few years a new method has emerged that poses a greater threat to the iOS ecosystem. Since 2013 it is possible to download free pirated versions of paid iOS apps from rogue iOS app stores without jailbreaking your phone through a process called backloading. This trend has evolved from a simple pirate site in China to what it is today, an explosion of international piracy app stores with a growing base of at least 10 million users with no sight in end for its growth. We will explore the history of backloading and the pirate industry it has created, its hazards, and solutions.

Definitions

To better aid in understanding, we have defined the terms needed for the purposes of our topic as follows.

·Sideloading : A method of installing an application through alternate sources other than traditional distribution methods (Google Play for Android, App Store for Apple, etc).

·Backloading : A subset of sideloading specific to the iOS that allows users to download illegal or pirated apps without the need of jailbreaking their phone.

·Jailbreaking : The act of modifying a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software. Also known as “rooting” for Android devices.

·IP Address : a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

·Disassembler : a program for converting machine code into a low-level symbolic language.

·Enterprise Certificate : A premium certificate issued by Apple to iOS app developers. Enterprise Certificates allow the developer to distribute apps without going through Apple’s App Store for use cases such as internal apps, private app distribution, etc. To obtain an Enterprise Certificate, the developer must be a registered business entity.

·Developer Certificate : A certificate issued by Apple to iOS app developers for signing mobile applications with their unique developer signature.

·Code Signing : Using your certificate issued by Apple within your app’s code to assure users that it is from the developer and the app hasn’t been modified since it was last signed.

·UDID : A unique device identifier (UDID) is a 40-character string assigned to Apple devices including the iPhone, iPad, and iPod Touch.

·Root Device or Rooting : The act of gaining root access, or master access, to your device, to bypass any hardware or mobile carrier restrictions that have been imposed. Rooting a device allows for enhanced privileges, such as running suspicious apps, or installing apps that are only available in other geographic regions.

·VPN : A VPN (virtual private network) creates a safe and encrypted connection over a less secure network, such as the internet. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods - including passwords, tokens and other unique identification methods - to gain access

·Nodes : Either a redistribution point (e.g. data communications equipment), or a communication endpoint (e.g. data terminal equipment).

·Riskware : Legitimate programs that can cause damage if they are exploited by malicious users – in order to delete, block, modify or copy data, and disrupt the performance of computers or networks.

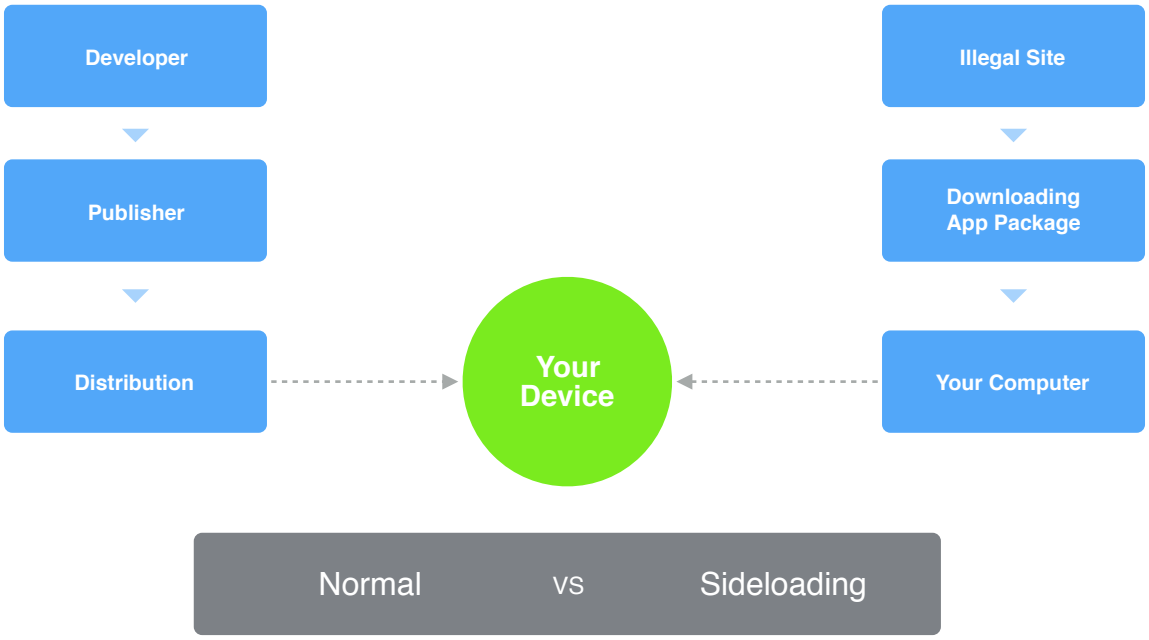
·Remote Access Trojans : A malware program that installs a backdoor for hackers to gain administrative control over the target computer or device. RATs are usually downloaded invisibly with a user-requested program, such as a game, or sent as an email attachment.

·Dark Web : the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. Generally used for illegal or malicious purposes like selling contraband ranging from people’s credit card information to drugs.

History of Backloading

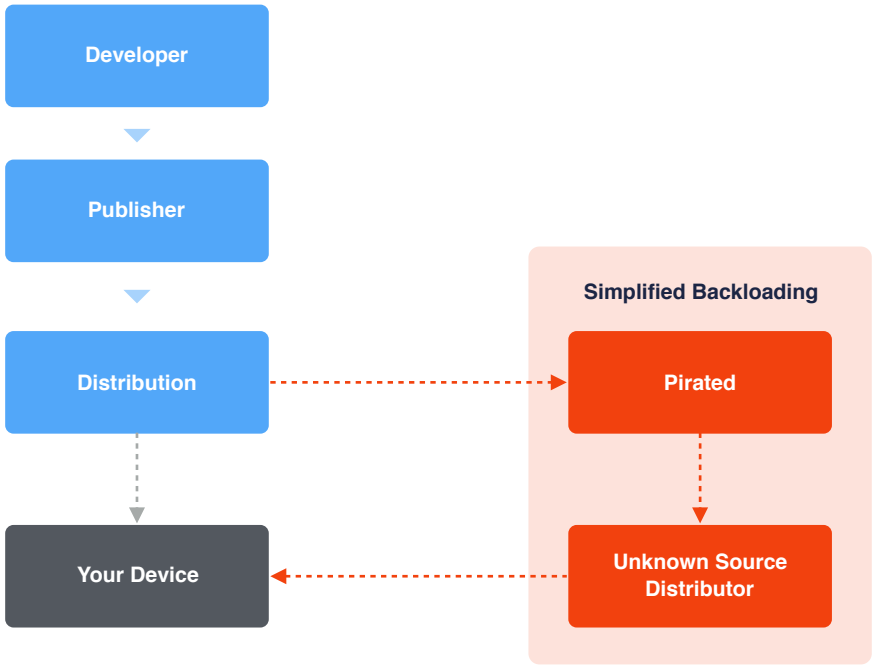
What is Sideloading?

Sideloading is when a mobile application is downloaded and installed on a mobile device without going through traditional app stores such as Google Play or the Apple App Store. The term is derived from downloading and uploading as the concept is similar but doesn't involve the normal method of installation.



Sideloading works

This has further evolved into backloading, which will be what this paper discusses in length. The execution of backloading is similar to sideloading with the major difference of not needing to be jailbroken on iOS to happen. It is only possible to backload apps if the user has allowed and trusted the "unknown sources" in their security settings.



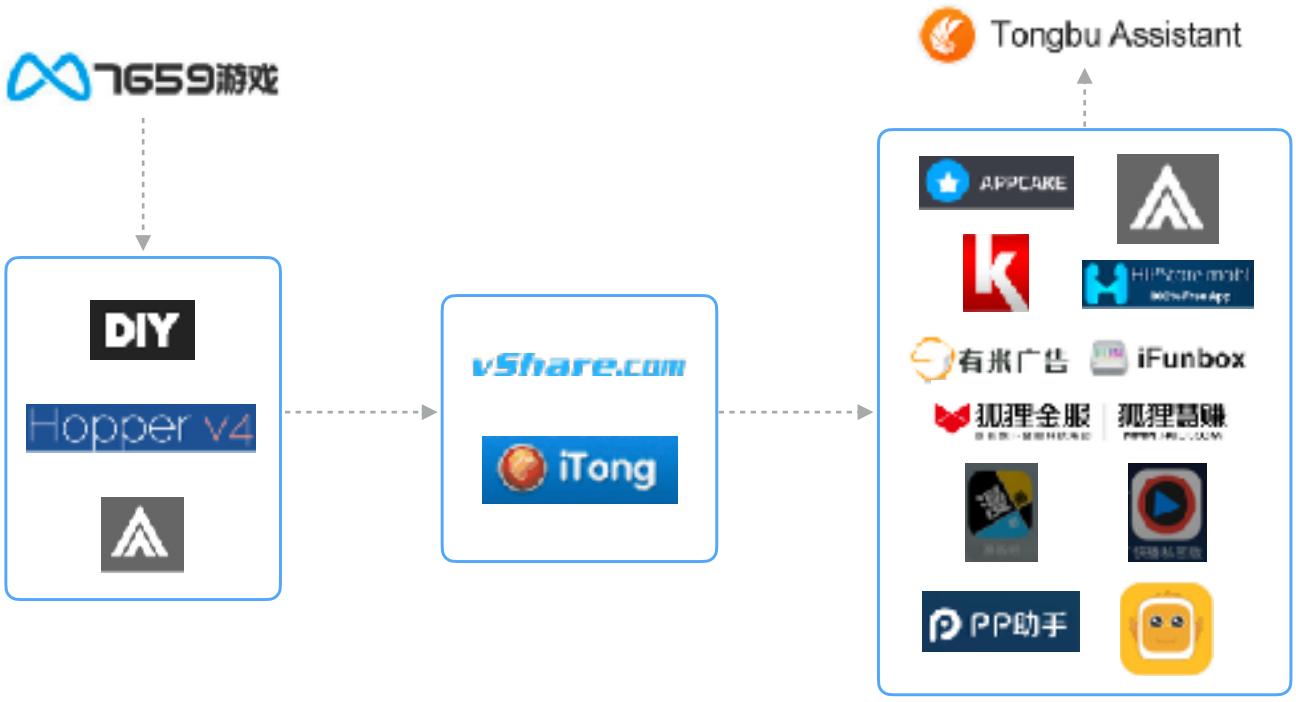
Backloading works

Infancy

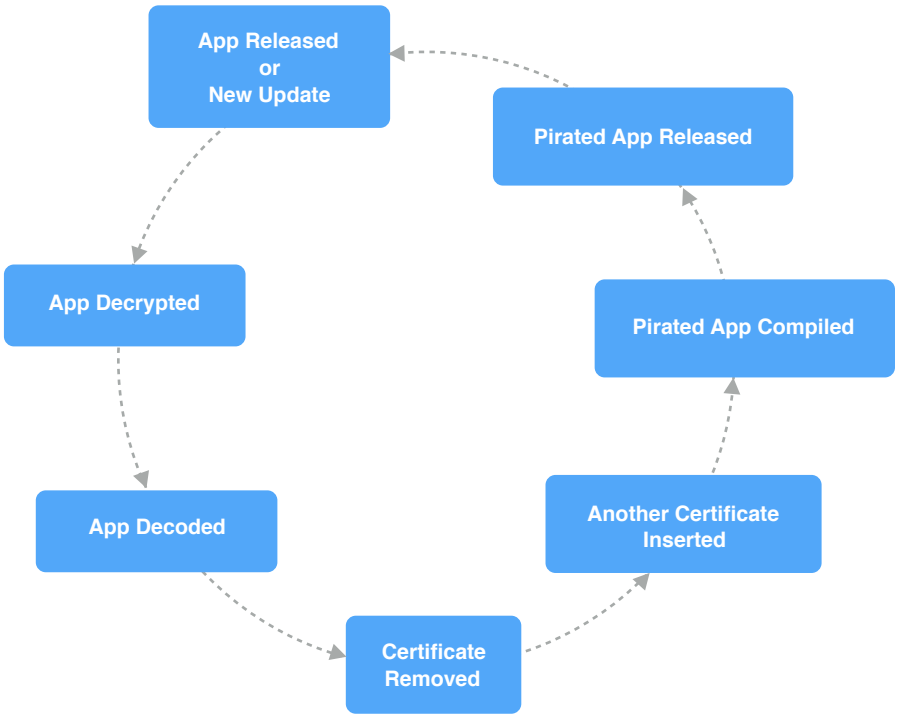
The first documented appearance of backloading, coined that for its use of back doors left in the iOS for distribution, can be traced back to the Chinese pirating site 7659.com in 2013. This was a Chinese company with a website only accessible to Chinese IP addresses, letting them remain under the radar and out of Apple's immediate reach. Each app on their site was found to have all been code signed with an enterprise certificate, allowing them to disperse the pirated apps outside of Apple's App Store. The defense for this website was that it allowed the large Chinese market to test out apps before purchasing them as well as to provide apps that were region locked and therefore not available to Chinese users.

Moving forward to 2014 we find that individuals willing to put in the extra work were able to provide pirated apps for others through online instructions. With the advent of software such as Hopper ($89) and Clutch High Speed iOS Decryption System came the resurgence of mass piracy. Though this was regulated to small isolated pools and black hat file sharing, this provided the base for the larger scale rogue app stores that would pop up in the following years.

Evolution



In the next two years we have seen a rapid evolution in backloading that seems to become more innovative at circumnavigating the obstacles that Apple tries to put in place. One of the most well know innovators is vShare with their DarkSideLoader marketplace. Using Apple's own enterprise certificate system to disperse pirated apps, vShare gathered large pools of these certificates that they'd switch out once Apple started cracking down on one. To do this they used three main methods: creating a fake company, impersonating a real company, or stealing an enterprise certificate from an actual company. To steal a company's enterprise code they would simply do what they were already doing within their piracy pipeline - decrypt and decode the app, and then snatch any certificate codes that were within the app. This information was readily available thanks to Apple's code signing policies.

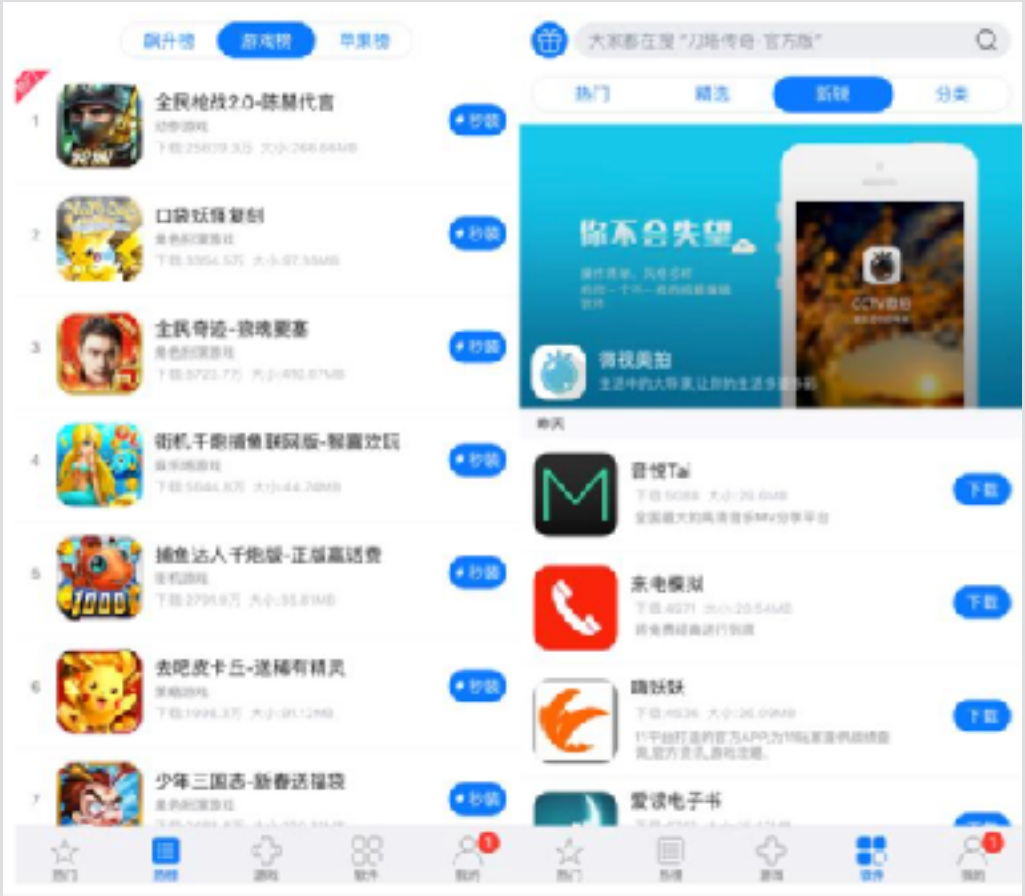


Certificate Snatch Diagram

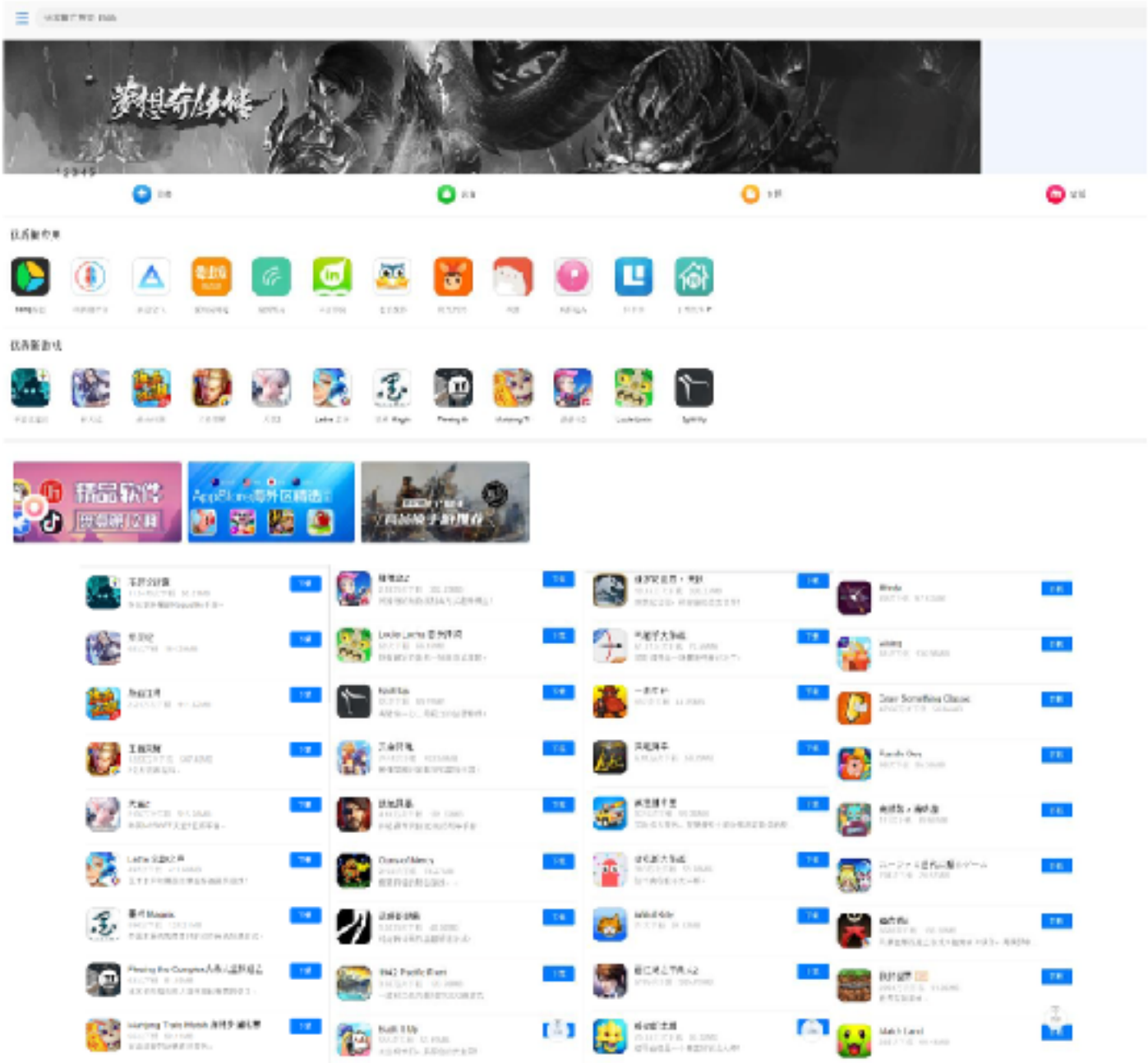
An interesting take in this matter was discovered when Tongbu and its assistant software iTong, their own personal version of Apple's iTunes, was discovered. Not only was it a rogue app store and a rogue desktop client companion software but it also allowed for pirated apps to receive the updates provided for legitimate versions of the app. Previously, app updates were only available for apps distributed through Apple's official app store, meaning that pirated versions would be on an older version, or would be rendered useless if the developer chose to force a download of updated versions and set up version checks on their server. iTong changed this landscape completely, setting up an entire pirating system that was equivalent to Apple's in every way AND allowed for all of the apps to be downloaded, even paid apps.

In 2016, the following year there was an even further explosion of unauthorized app stores utilizing backloading techniques such as WireLurker, YiSpecter, Youmi, HipStore, AppCake, AppAddict, KuaiYoung, iFUNBOX, m.huli.cn, Happy Day English, 25PP, and more. The two most interesting to note from this list are Happy Day English and 25PP because of their approach in circumnavigating Apple's App Store.

To anyone outside of China, Happy Day English was a mobile app used to help learn English and improve your English skills. It could be simply downloaded from the official App Store. However, the app came with hidden software embedded inside called ZergHelper that contained functions to circumvent Apple's security restrictions. For anyone outside of China, it acted like a normal mobile app. For anyone in China, this app took an interesting turn and became a massive rogue app store that even came with its own augmented version of Apple's iTunes client application. Through the use of Lua's "wax" (a framework used to create apps on iOS) it dynamically updated the apps' code, getting around the Apple review process, and gave users updated versions of apps that were previously unavailable to jailbroken devices. They even reverse engineered the Xcode to generate unauthorized developer certificates for free.



Like vShare, a mobile-accessible website that allowed users to download pirated mobile apps, 25PP operates as a website. It takes things one step further, however, and allows users to directly download apps through their mobile device. After following their download instructions, a rogue app store is installed on your phone. Through 3 different icons and profiles on your phone you are given access to a global pirated app market that includes big names such as MineCraft, Need for Speed, and Final Fantasy.



Current Iterations

App piracy is an ongoing problem that will never fully disappear, despite best efforts. On the contrary, it's an ever-growing market. There are more and more rogue app stores popping up that allow for users to get around paying for an app, some of which also provide your updates automatically to the pirated product. Though white hat hackers are working tirelessly in tandem, and often with Apple, to stop this, the endless number of differing systems and workarounds turn up new methods of backloading every day. No system is ever perfect, and vulnerabilities will always exist. Tongbu/iTong hasn't gone anywhere but has instead rebranded itself as Tongbu Assistant, a management program for iOS and Android phones that also happens to provide paid apps for free for a small monthly subscription. There are also now at least 20 rogue duality app stores like 25PP out there, even more sites like vShare, and possibly countless apps that have secret access tied to physical locations like the Happy Day English app that have yet to be discovered.

Dangers of App Piracy

Security Risks to the User

Rooting (or “jailbreaking”) a mobile device means more customizable options and access to apps that may not have been available previously, but it comes at a cost. By removing restrictions imposed by Apple and/or hardware manufacturers and carriers, you also strip away security restrictions. The default root password for Apple devices is well known - rooting your device means you are one potential and quick Google search away from anyone who wants direct access to your information. With the new generation of rogue app stores and apps, the risks get larger. Previously the only way to install a pirated app was to root your phone; now that is not a hard requirement. When you download an app from a rogue app store you risk exposure to embedded code that may give anyone unauthorized access to your device without your knowledge or consent.

Pirated apps may contain malicious code (also known as malware) that can lead to serious consequences. Choosing to trust the "Unknown Source," which is a requirement for downloaded pirated apps, can give these apps more permission that you think. These apps can transmit sensitive user data, sometimes hijacking this information from other apps installed on your device, to third party malicious sites that than exploit or resell your information for profit. Your device is in open and active communication with people that have the programming knowledge and experience to do some major digital theft. How much data is being sent back and how much monitoring of your activity they are doing is completely unknown. This can be a problem because it can access any information it wants on your phone as you’ve already given it permission through telling your device to trust its source. This allows it to aggregate things like your banking info, PayPal details, emails, account information and more. All of which lead to possible financial loss and identity theft.

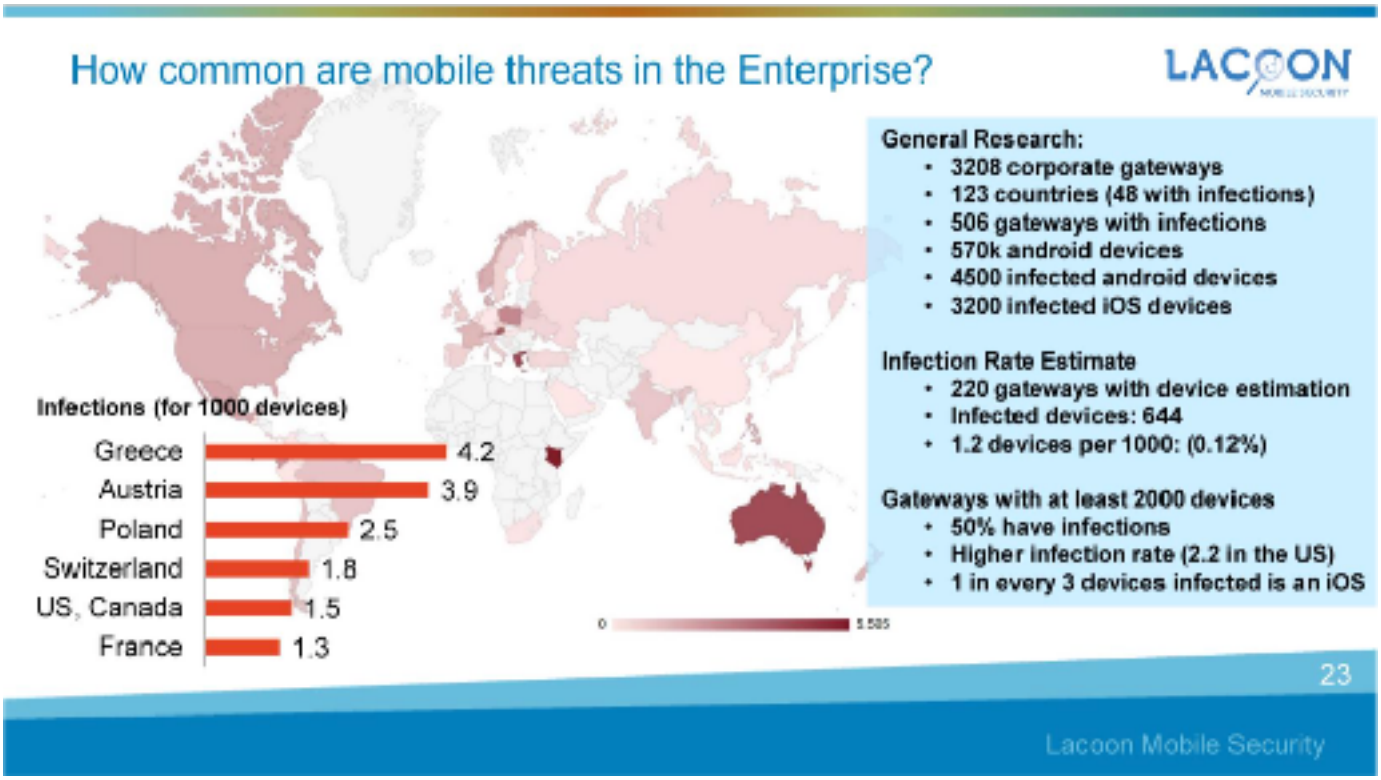
Malware can also hijack your hardware device and use it to run unauthorized processes, like downloading apps, running ads in the background, acting as ransomware, and installing viruses like trojan horses that become difficult to remove. It can also send and receive premium SMS messages, running up unwanted charges on your phone bill.

In most cases, a rogue app store installation requires the creation of multiple configuration profiles. You are essentially handing over the keys to the program and its creators to control access to everything from WiFi, VPNs, email, your calendar, passwords and your device’s restrictions. This gives the person, or group, behind the massive rogue app the ability to gather astronomical amounts of data about you. If you are like most everyone on the planet who ends up accessing work emails and documents on the go via your smart phone, this also opens the company up to having all of its data taken as well. After gathering all this data if they so choose they could use the new profile to redirect you to targeted malicious sites that are more likely to work given their knowledge of you as a digital user, causing its own set of security problems.

Risks to Enterprises

As discussed in length in this Dangers of App Piracy section these rogue app stores, and the ability to sideload pirated apps, presents huge security risks for companies. An employee making a decision to negate embedded security features on their mobile device opens up the entire internal network to a host of attacks, scams, security breaches, and data leaks. According to MixRank, there are 1223 iOS apps with exposed RSA private keys, allowing an attacker to take control of the company's servers. New apps with vulnerabilities pop up daily, and MixRank has reported 8 new discoveries in one day. No one is immune, and MixRank reports apps developed by 7 of the Fortune 500 to be affected. No amount of network security can completely protect against it. For this reason, no mobile device can be considered secure unless it is actively running forms of mobile security in conjunction with the established internal network security. A single infected mobile device can cause ramifications felt by the entire company.

Targeted attacks on mobile devices are now easier than ever. One major threat is mobile remote access trojans (mRAT), a virus that installs itself into the mobile device to give hackers access to data, apps and the hardware device. These viruses can also further infect other devices in the network, if two or more devices connect to a common network or to each other. A lot of rogue app stores either build mRATs into their store, downloading them quietly in the background once the user has granted access to the unknown source, or embed them into the downloaded pirated apps. A research study done in 2015 by Lacoon Mobile Security found that on average 0.15% of mobile devices were found to be infected with mRATs. Furthermore, the infected devices went on to compromise 0.31% of total devices, doubling the damage. While this may not seem like a lot, the number of compromised devices can continue to grow if left unchecked, and it only takes one device being compromised to create a security breach. Possible scenarios include tracking device locations, installing key loggers, taking screenshots, getting into calendars and emails, taking passwords, listening in on calls and more. This creates a potential scenario of massive risk and damage, financial and otherwise, to the company, with minimal infection rates.



Post-download, rogue app stores and their pirated apps often have the ability to change and reconfigure the permissions given to them and other downloaded apps. This nefarious action can lead to all sorts of problems. Suddenly it can allow them access to your location services, contacts, network settings and connections. On an individual scale it's concerning; when magnified to a company scale, it can be catastrophic. One employee with a compromised mobile device can suddenly give hackers access to any documents they view on their phone, any file sharing services they use to work, and any emails that they may send or receive. All of this is done without the user's knowledge, and it can be months or years before the breach is discovered, leading to countless data leaks. Even when caught and addressed, these rogue app stores and their pirated goodies still retain the trusted status and permissions, meaning they can re-infect the device and organization at any given time.

The seemingly harmless consequence of having traffic redirected to a controlled node could have big repercussions. Passing your request for network connections and traffic through a node of their choosing allows them to sniff through your data looking for anything worth taking. While this is a more passive data breach then most of the others discussed in this particular subsection it can still lead to a loss of informational security within a company if even a single mobile device connected to their internal networks is infected. In a worst case scenario, a hacker could then follow the flow of information backwards and into internal network systems to cause further damage.

It's not scary enough that free apps can suddenly mean a massive data breach and loss of security for your company. Often times these rogue app stores will use the data they've gathered and sell it off to make a profit. Or worse sell off a back door into the mobile device for whoever else wants to get into it and cause some chaos. This means that sensitive information vital to your company's wellbeing and continued existence could be up for grabs on the dark web, possibly even sold for less than a meal in San Francisco if you managed to scoop it up before its value was realized. Normally these sorts of data sales are done in massive dumps, multiple terabytes of data all bundled together. So sorting through it to find the valuable stuff would take time and patience, but even that hurdle is growing smaller and smaller as commercially available software to help manage these massive data dumps becomes available to the mass market.

Backloading's Impact to the Developer

With the new growing pirating avenue, every major app on the iOS market is a potential honey pot for riskware. Should someone's information, money, identity, and digital life be stolen and destroyed, it would be a major blow to the original developer. Even though it was a pirated version that caused the security breach, users would place the blame on the name and branding attached to the original app. This can cause untold losses in consumer trust and brand loss, and publishers and developers must take steps to protect themselves immediately.

The most immediate impact felt by backloading is lost revenues and users - with every person installing an unsanctioned version of a mobile app, that is potential revenue that the developer cannot collect. Market cannibalization occurs on both an app store and geographical scale, because the apps are intruding into existing markets through unsanctioned app stores, and publishing unauthorized apps in markets where the original developer has yet to release their product. By the time the developer releases the product into a new market, the copycat may have already saturated and conquered the user base.

A secondary consequence is through security breaches that may lead to the leak of sensitive user information. A study published in 2014 looked at matching market value and market capitalization losses against security and data breaches at companies. It was found that after an announcement of a breach that, on average, announcing companies lost 2.1 percent of market value, which equals about $1.65 billion lost per breach. For a smaller company, this could be catastrophic. These breaches cause a massive loss of customer and public trust. Once that trust is broken, we see the corresponding dip in market values and capitalization as users move on to other services that claim better security. With everybody doing so much work, finances, shopping and more from their mobile devices, the need for mobile security on the app level to protect the reputation of the company and public trust grows exponentially as well.

Conclusions

Fight Back with Security

The first line of defense should always be proactive actions during the development process to protect against security threats. Incorporating security measures from the beginning can greatly decrease the risk of an app being compromised. Mobile security, while an emerging field, has some heavy contenders when it comes to protecting mobile applications against hacking threats. One of the most powerful measures a developer can take is to secure the mobile application at the source code and binary level - by presenting the hacker with deterrents and obstacles, this creates a compelling reason for them to change their target to another application or developer.

AppSolid for iOS is a mobile security service provided by SEWORKS. Designed as an easy to use tool for app developers, it works as a custom compiler inside the Xcode development environment. Other solutions provide security features via shared library files, which become a liability because shared libraries must contain function names in their symbol table which cannot be deleted. When a hacker analyzes the mobile app and discovers strings containing words like “integrity” or “jailbreak,” the function containing the strings can be discovered, making it easier for attackers to bypass security features. AppSolid’s iOS protection module is automatically inserted into the app at build time and automatically loads when the app is launched. This generates random code for every build, making it extremely difficult to break through any or multiple layers of AppSolid’s security suite through analysis. By creating more work and more layers of difficulty, the payout is less compelling for hackers who can shift their resources to easier hacking targets.

The AppSolid iOS tamper check uses a method that is not affected by problems using a hash value check method (hash collision, bitcode, etc). To increase the effectiveness of the tamper check, both in-memory and in-filesystem check methods are used. It is checked both statically and dynamically to ensure the integrity of an app’s binary. AppSolid’s system uses multiple prongs of validation and checks to detect, mitigate, and protect against an attacker before and during runtime. This part of the service helps to keep pirated apps out of circulation by combatting the process of changing the apps’ originally intended code.

To protect against cases where the anti-debugging measures are bypassed, the debugger detection routine runs at app launch until the app is closed. Should an attacker try to launch the app with a debugger, the app terminates at a random time, to make it harder to identify when and where in the code the termination is called. If the attacker tries to attach to the process with the debugger, then the debugger itself will crash. This protective casing and offensive defense keeps the attackers from ever having a chance to dig into your code, find points to manipulate it, steal information from it, and augment it to their needs, cutting off the process by which these pirated apps are churned out before it even gets started.

All of the features above could be defeated with a lot of time and effort through static analysis if an attacker was determined to unravel a particular app. AppSolid has thought of this and added obfuscation to harden the binary statically against such analysis. The three biggest and most beneficial ways this is achieved are through control flow obfuscation, cross reference removal obfuscation, and string encryption. Combined with the rest of the detailed obfuscation AppSolid provides for iOS apps this makes the work extremely daunting and unfavorable for an attacker.

Summary

There is a massive ever growing market of pirated apps out there, and the trend isn't slowing down anytime soon. The cost of having a pirated app on a mobile device is high for all involved from the mobile device user, to their workplace, and even the developer of the original app. In order to combat the chances of this happening we need to be focused on mobile security from the app up. The easiest way to stem the growth of these established pirating venues is to stem the flow of useable pirated apps. To do this, developers and publishers need to take the first steps towards making sure their apps, whether developed for the open market or for internal distribution, are protected with the highest level of professional mobile security available. This will prevent apps from appearing on pirating marketplaces in the first place. A leading provider in the area of mobile security is SEWORKS with their AppSolid product, which is a powerful and easy to use solution. It is our recommendation that anyone serious about protecting their app from attackers needs to secure the mobile app client and consider outside solutions like AppSolid.

References

P. (2016, November 15). Top Vshare Alternative Apps for iOS: No Jailbreak Required. Retrieved May 30, 2017 from https://www.progeeksblog.com/apps-like-vshare-alternative/

[huli china app for iOS 10/9/8] Download Paid Apps and Games free without Jailbreak No Apple ID. (2016, November 13). Retrieved May 30, 2017 from https://www.youtube.com/watch?v=AMJnb-XwwbY

Misuse of enterprise and developer certificates. (n.d.). Retrieved May 30, 2017 from https://www.theiphonewiki.com/wiki/Misuse_of_enterprise_and_developer_certificates

Download 25PP iPhone & iPad App Without Jailbreak. (2017, April 22). Retrieved May 30, 2017 from https://www.unlockboot.com/download-25pp-iphone-ipad-app-without-jailbreak/

Xiao, C. (2016, February 21). Pirated iOS App Store's Client Successfully Evaded Apple iOS Code Review. Retrieved May 30, 2017 from http://researchcenter.paloaltonetworks.com/2016/02/pirated-ios-app-stores-client-successfully-evaded-apple-ios-code-review/

Cimpanu, C. (2016, January 08). Rogue iOS App Stores Expand from the Chinese Market to the Whole World. Retrieved May 30, 2017 from http://news.softpedia.com/news/rogue-ios-app-stores-expand-from-the-chinese-market-to-the-whole-world-498632.shtml

DarkSideLoader: Rogue App Stores Targeting Non-Jailbroken iOS Devices. (n.d.). Retrieved May 30, 2017 from https://www.proofpoint.com/us/threat-insight/post/DarkSideLoader-Rogue-App-Stores-Targeting-Non-Jailbroken-iOS-Devices

Get Paid Apps For Free Without Jailbreak On iPhone. (2015, November 25). Retrieved May 30, 2017 from http://technobrij.com/get-paid-apps-for-free-without-jailbreak-on-iphone/

Koretsky, D. (n.d.). Practical Attacks against Virtual Desktop Infrastructure (VDI) Solutions. Retrieved May 30, 2017 from https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf

Jha, S. (2017, January 01). Get paid apps for free in iOS9 without Jailbreak via Tongbu. Retrieved May 30, 2017 from http://techglobule.com/2015/05/tongbu/

Get Paid IOS Apps For Free Without Jailbreak! 2017. (2013, November 24). Retrieved May 30, 2017 from https://www.youtube.com/watch?v=ZcQZTOTMTAI

Zdziarski, J. (n.d.). How App Store Apps are Hacked on Non-Jailbroken Phones. Retrieved May 30, 2017 from https://www.zdziarski.com/blog/?p=4002

Chinese 'app store' lets you install pirated iPhone apps — without jailbreaking. (2013, April 18). Retrieved May 30, 2017 from https://venturebeat.com/2013/04/18/chinese-app-store-using-apples-own-enterprise-app-distribution-tech-to-distribute-pirated-apps/

James Plafke on April 19, 2013 at 1:10 pm Comment. (2013, April 19). Chinese app store offers pirated iOS apps without the need to jailbreak. Retrieved May 30, 2017 from https://www.extremetech.com/mobile/153849-chinese-app-store-offers-pirated-ios-apps-without-the-need-to-jailbreak

ZergHelper. (n.d.). Retrieved May 30, 2017 from https://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas/ZergHelper/detailed-analysis.aspx

Mobile Data. (n.d.). Retrieved May 30, 2017 from https://mixrank.com/datasets/mobile

The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. (n.d.). Retrieved May 30, 2017 from http://www.tandfonline.com/doi/abs/10.1080/10864415.2004.11044320

Remote Access Trojan (RAT). (n.d.). Retrieved May 30, 2017 from https://blog.malwarebytes.com/threats/remote-access-trojan-rat/

Creese, D. M., & Robert D. Austin and Christopher A.R. Darby. (2014, October 24). The Danger from Within. Retrieved May 30, 2017 from https://hbr.org/2014/09/the-danger-from-within

Is nothing sacred? Risky mobile apps steal data and spy on users. (n.d.). Retrieved May 30, 2017 from https://www.proofpoint.com/us/threat-insight/post/Risky-Mobile-Apps-Steal-Data

Hoffman, C. (2013, November 24). Why Configuration Profiles Can Be As Dangerous As Malware on iPhones and iPads. Retrieved May 30, 2017 from https://www.howtogeek.com/176195/why-configuration-profiles-can-be-as-dangerous-as-malware-on-iphones-and-ipads/

Brodie, D., & Shaulov, M. (2014). Practical Attacks against Virtual Desktop Infrastructure (VDI) Solutions. Retrieved May 30, 2017 from https://www.blackhat.com/docs/us-14/materials/us-14-Brodie-A-Practical-Attack-Against-VDI-Solutions-WP.pdf