Lookout

Whitepaper

Enterprise Mobile Threat Report

The State of iOS and Android Security Threats to Enterprise Mobility

I. Introduction

This report examines enterprise security threats for iOS and Android. While Android has higher consumer market share, iOS commands more market share in the enterprise, accounting for 72% of enterprise mobile activations in Q1 2015 compared to Android's 26% activation share[1].

The perception that iOS is more secure has helped drive its enterprise adoption, but this perception comes largely from security trends observed in the consumer space. Android, with a more open mobile platform and 81% global market share[2], predictably invites more broad-based attacks than iOS.

When it comes to iOS and Android in the enterprise, however, both need threat protection because at a fundamental level both platforms are subject to similar vulnerabilities and attack methods. iOS attacks may be relatively uncommon today, but they have happened and can occur. Moreover, enterprises increasingly rely on iOS app-distribution methods that forgo Apple's app-review and they face the risk that attackers will continue to abuse this distribution process to deliver malware directly to devices.

To summarize the current state of iOS and Android security threats to enterprise mobility:

iOS security threats consist of malicious uses of enterprise provisioning methods that bypass Apple's app-review and deliver malware directly to target devices, as well as OS vulnerabilities and jailbreaks that compromise OS integrity and device security.

Android security threats consist of prevalent and increasingly more sophisticated malware attacks, as well as OS vulnerabilities that put enterprise data at risk by facilitating device compromise.

II. iOS Security Threats

App Threats

Through rigorous app-review, Apple has done an outstanding job and brought the risk of downloading malware from its App Stores to near zero. iOS attacks to date, however, have largely come from outside Apple's review and App Store distribution. These attacks have targeted both jailbroken and non-jailbroken devices, targeting the latter by abusing an app distribution method Apple offers to companies that enables app installation without requiring app review or App Store distribution.

Apple created this app distribution method, known as enterprise provisioning, so that companies can easily distribute custom apps to their employees.

[1] "Mobility Index Report Q1 2015". Good Technology. May 2015. https://media.good.com/documents/mobility-index-report-q1-2015.pdf

[2] "Android Shipped 1 Billion Smartphones Worldwide in 2014". Strategy Analytics. January 2015. http://www.prnewswire.com/news-releases/strategy-analytics-android-shipped-1-billion-smartphones-worldwide-in-2014-300027707.html

Apple has implemented two security mechanisms designed to stop unchecked abuse of the process: app certificate validation and device security notices.

To run on a device, enterprise-provisioned apps must be signed using an Apple-issued signing certificate. Apple provides signing certs to approved developers through its Enterprise Developer Program, requiring only proof of a registered business (i.e. a D-U-N-S number) and a yearly $299 payment. Unfortunately, attackers have circumvented this process by registering legal entities to obtain a certificate or by using certificates Apple has issued to other parties.

When Apple learns of enterprise provisioning abuse it promptly revokes the certificate, as was the case with MacBuildServer.[3]

It's difficult, however, to keep tabs on this problem given the growth of enterprise provisioning. Security researchers recently documented more than 1,000 iOS apps available for public download outside the App Store that used either enterprise or developer certificates.[4] Developer certificates (meant for app testing) enable signed apps to run on up to 100 pre-selected devices, while apps signed by enterprise certificates can run on an unlimited number of iOS devices.

Apple also provides device security notices when installing enterprise-provisioned apps. The notice warns the user that the developer is unknown and asks them if they wish to proceed. Unfortunately, the ubiquity of legitimate enterprise-provisioned apps has conditioned employees to seeing (and ignoring) these security notices, making it likely that many would accept and install a maliciously provisioned app.

Table 1: iOS Threat Discoveries 2014-2015

Threat	Year	Description	Target
XAgent (i.e. Operation Pawn Storm)	2015	XAgent is iOS surveillanceware that collects a range of sensitive data from compromised devices including SMS, contacts, photos, and GPS locations. It can also remotely activate audio- recording functionality on compromised devices.[5]	• Non-jailbroken devices via enterprise provisioning abuse • Jailbroken devices
Xsser mRAT	2014	Xsser mRAT is an iOS remote access trojan, with the potential to spread through man-in-the-middle and phishing attacks. Xsser mRAT steals data from and can execute remote commands on compromised devices.[6]	• Jailbroken devices
WireLurker	2014	Wirelurker is iOS surveillanceware delivered via USB connections to infected OS X devices. Wirelurker can capture contacts and SMS messages from compromised devices.[7]	• Non-jailbroken devices via enterprise provisioning abuse • Jailbroken devices

[3] "Apple Slams The Door On Super Mario". ReadWrite. July 2013. http://readwrite.com/2013/07/17/apple-slams-the-door-on-super-mario

[4] "Enpublic Apps: Security Threats Using iOS Enterprise and Developer Certificates". Zheng, Min, Hui Xue, Yulong Zhang, Tao Wei, and John C.S Lui. April 2015. http://www.cs.cuhk.hk/~cslui/PUBLICATION/ASIACCS15.pdf

[5] "XAgent iPhone Malware Attack Steals Data without Jailbreaking". MacObserver. February 2015. http://www.macobserver.com/tmo/article/xagent-iphone-malware-attack-steals-data-without-jailbreaking

[6] "Xsser mRAT Targets iOS and Android for Man-in-Middle Attacks". Akamai. December 2014. https://blogs.akamai.com/2014/12/ios-and-android-os-targeted-by-man-in-the-middle-attacks.html

[7] "Malicious Software Campaign Targets Apple Users in China". The New York Times. November 2014. http://bits.blogs.nytimes.com/2014/11/05/malicious-software-campaign-targets-apple-users-in-china/?_r=0

Continued - Table 1: iOS Threat Discoveries 2014-2015

Threat	Year	Description	Target
Unflod	2014	Unflod is an iOS threat that monitors SSL connections in an attempt to steal the device's Apple ID and password.[8]	Jailbroken devices
AdThief	2014	AdThief is an iOS threat that hijacks specific ad SDKs to redirect mobile ad revenue away from legitimate ad networks to the attackers.[9]	Jailbroken devices

OS Vulnerabilities

In addition to app-based threats, operating system vulnerabilities in outdated iOS devices also pose an enterprise security risk. For example, **39% of iOS devices currently use an outdated OS** (8.2 or earlier - see Figure 1)[10], potentially exposing these devices to a wide range[11] of vulnerabilities patched in the iOS 8.3 update, such as:

- A vulnerability that could allow remote attackers to execute code on the device, delivered through a malicious website.[12]
- A vulnerability that could enable a malicious app to guess a user's device passcode.[13]

In addition, 13% of iOS devices use an OS version vulnerable to Masque Attack (7.1.1, 7.1.2, 8.0, and 8.1), an exploit that could enable attackers to compromise non-jailbroken devices via enterprise provisioning abuse, replacing legitimate apps with trojanized versions while evading detection.

Figure 1: Operating System Version Distribition for iOS

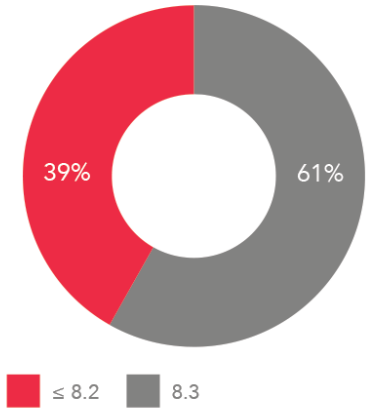
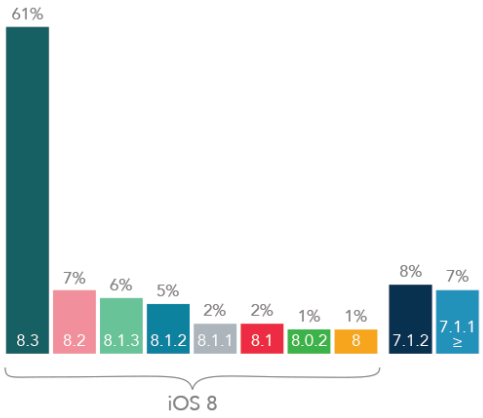


Figure 2: Operating System Version Distribition for iOS



[8] "iOS Malware Campaign "Unflod Baby Panda". SektionEins. April 2014. http://www.sektioneins.com/en/blog/14-04-18-iOS-malware-campaign-unflod-baby-panda.html

[9] "Threat Post: Malware on iOS is Ad Thief". Mobile Advertising Watch. September 2014. http://mobileadvertisingwatch.com/threat-post-malware-ios-ad-thief-11402

[10] Source: MixPanel, iOS version distribution as of May 12th, 2015. https://mixpanel.com/trends/#report/ios_frag/

[11] "Apple's Colossal iOS 8.3 Update Kills 58 iOS Security Bugs". The Mac Security Blog. April 2015. http://www.intego.com/mac-security-blog/apples-colossal-ios-8-3-update-kills-58-ios-security-bugs/

[12] CVE-2015-1088. See: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1088

[13] CVE-2015-1085. See: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1085

Jailbreak Threats

Jailbreaking removes hardware restrictions on the iOS operating system and many iOS users, estimated to be nearly 8% globally, intentionally jailbreak their device to access restricted content and device functionality and enable extended customization. Jailbreaking, however, compromises the integrity of the operating system and can make security technologies such as containers, which depend on the operating system, vulnerable to attack. Unfortunately, individuals can easily evade standard jailbreak detection methods using free tools such as xCon[14] or FLEX[15]. With tens of millions of devices jailbroken to date, the prevalence of this threat makes jailbreaking a substantial risk to enterprise security.

Jailbreak Stats

- **Approximately 8% of all iPhones (over 30 millions devices worldwide) are jailbroken[16]**
- **Cydia (a popular 3rd party app store) claims over 20 million installations and contains thousands of apps available for download[17]**
- **Within a week of its release in 2013, the evasi0n jailbreak tool was used to jailbreak more than 7 million iOS devices[18]**

III. Android Security Threats

App Threats

Lookout analyzed mobile threat encounters from more than 20,000 Android devices associated with 25 different Fortune 500 companies[19] and found that these devices have encountered 233 different app-based threat families. These threats ranged in severity from adware-caused data leakage, to sophisticated trojans like NotCompatible, a proxy botnet that could enable attackers to compromise secure networks.

Key threat insights obtained from this sample of enterprise devices include:

- These enterprise devices had **10 NotCompatible encounters per 1,000 devices.**
- These **enterprise devices encountered 11 different root enablers** that could compromise OS security features and put enterprise data at risk.

[14] See: https://theiphonewiki.com/wiki/XCon

[15] See: http://www.sinfuliphone.com/showthread.php?t=10032183

[16] WireLurker" Malware May Have Infected 100,000+ iPhones, No Jailbreak Required". Daily Tech. November 2014. http://www.dailytech.com/WireLurker+Malware+-May+Have+Infected+100000+iPhones+No+Jailbreak+Required/article36850.htm

[17] "Over 20 Million iOS Devices Running Cydia". iPhone Hacks. January 2013. http://www.iphonehacks.com/2013/01/20-million-jailbroken-devices-cydia.html

[18] "Evasi0n Is The Most Popular Jailbreak Ever: Nearly Seven Million iOS Devices Hacked In Four Days". Forbes. February 2013. http://www.forbes.com/sites/andy-greenberg/2013/02/08/evasi0n-is-the-most-popular-jailbreak-ever-nearly-seven-million-ios-devices-hacked-in-four-days/

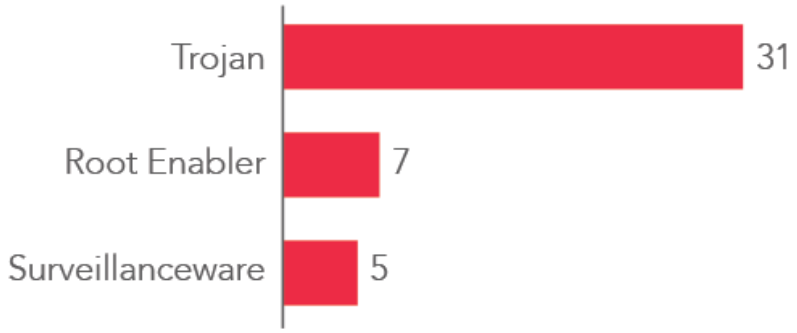
[19] Methodology: Lookout analyzed the threat detection data from its consumer security client, Lookout Mobile Security, which has millions of users worldwide. Lookout correlated device IP connections to publicly-available Autonomous System Numbers (ASN) to show where these devices may have connected to the corporate networks of one of 25 different Global Fortune 500 companies.

- These **enterprise devices encountered over 25 different types of surveillanceware** capable of committing comprehensive data exfiltration from compromised devices. The top three most common surveillanceware threats detected among these devices were:
    - **MSpy** - captures a range of data, including SMS and emails, and can even remotely record ambient audio by activating the device's microphone.
    - **SMSTracker** - captures a range of data, including call logs, GPS locations, and SMS messages.
    - **BasicSystemSpy** - captures a range of data, including device contacts and browsing history.

Figure 3 below shows the yearly threat encounter rates for these devices across three mobile threat classifications of particular concern to enterprises:

- **Root Enablers** - Apps that gain root access to the Android OS, escalating a user's administrative privileges. Rooting can make devices more vulnerable to malicious attack.
- **Surveillanceware** - Apps that remain invisible on the device while surreptitiously engaging in comprehensive device monitoring and data exfiltration. They are typically directly installed by someone with physical access to the device.
- **Trojans** - Apps that advertise legitimate functionality, but surreptitiously perform malicious actions in the background, such as data exfiltration or billing fraud.

Figure 3: Enterprise Device Threat Encounter Rates



Yearly Encounters per 1,000 Devices

OS Vunerabilities

Operating system vulnerabilities in outdated Android devices also pose an enterprise security risk. For example, **nearly 1 in 3 devices use Android 4.3 or older[20],** which, if left unpatched, could expose them to at least two serious security vulnerabilities affecting these devices:

- **AOSP Browser Vulnerability:** Affects mobile browsers using the Android Open Source Project's (AOSP) browser code. This vulnerability could allow attackers to direct victims to a malicious webpage and access data in other open webpages in the browsing session, even taking control of an online account that a victim has logged into on another webpage. The vulnerability has a CVSS score of 7.5, requiring very little knowledge or skill to successfully exploit.[21]
- **MasterKey Vulnerability:** An Android OS vulnerability that allows attackers to modify .apk files (apps) without breaking their cryptographic signature, giving attackers the ability to maliciously update apps on devices and evade detection on devices with vulnerable OS versions. The vulnerability has a CVSS score of 9.3; while this vulnerability is rated at medium level access complexity, once exploited it results in a total compromise of system integrity.[22]

Figure 4: Operating System Version Distribition for Android

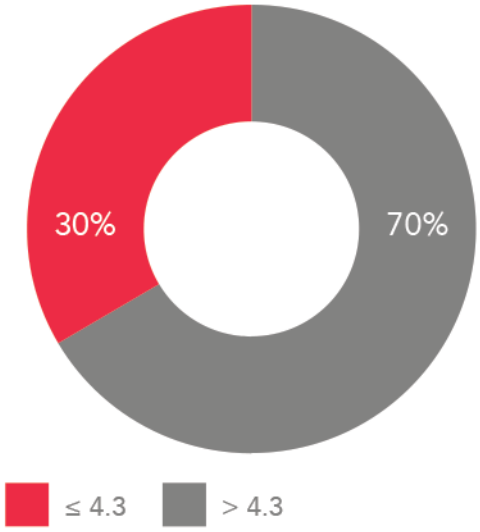
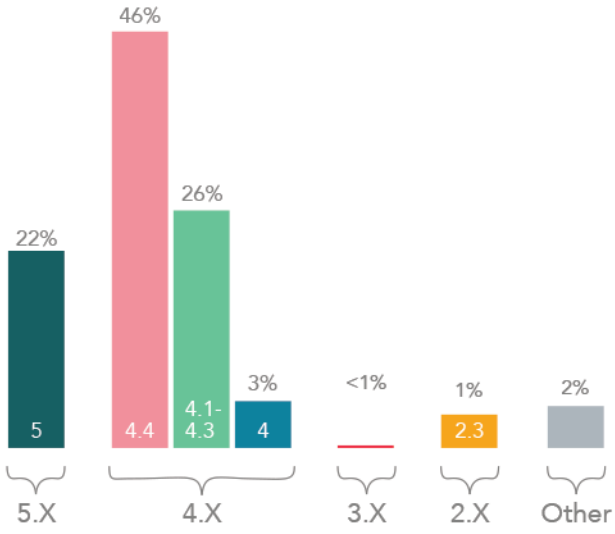


Figure 5: Operating System Version Distribition for Android



[20] Source: MixPanel, Android version distribution as of May 12th, 2015. https://mixpanel.com/trends/#report/android_os_adoption

[21] CVE-2014-1939. See: http://www.cvedetails.com/cve/CVE-2014-1939/

[22] CVE-2013-4787. See: http://www.cvedetails.com/cve/CVE-2013-4787/

IV. Conclusion

In summary, both iOS and Android can be the victim of targeted attacks. Both platforms suffer from security vulnerabilities and can be exposed to similar attack methods.

- iOS security threats today consist of malicious uses of enterprise provisioning to deliver apps directly to target devices, as well as OS vulnerabilities and jailbreaks that compromise device security. While iOS has effectively no broad-based malware attacks compared to Android it may well be at elevated risk of targeted attack given its dominant enterprise market share, which offers attackers a higher ROI.
- Android security threats today consist of prevalent and increasingly more sophisticated malware attacks, as well as OS vulnerabilities that put enterprise data at risk by facilitating device compromise. Android malware is a real and prevalent phenomena: for example, Lookout's analysis of 20,000 devices associated with major enterprises revealed 5 surveillanceware encounters per 1,000 devices.

A study conducted last year found that the cost of a corporate data breach grew 15% year over year, now averaging $3.5 million per victimized organization[23]. The rise of mobile computing has pushed sensitive corporate data far beyond the traditional, firewall-protected perimeter, and mobile devices now represent an increasingly attractive attack surface. Enterprises have learned to manage these devices using MDM, but most devices have only basic security protection in the form of encryption technologies that are dependent on operating systems, which themselves can be compromised through sophisticated attacks. With people now spending more Internet-connected time on mobile devices than traditional computers[24], security professionals need to approach corporate security from a mobile-first perspective.

[23] "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis." Ponemon Institute. May 2014. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

[24] "The U.S. Mobile App Report". comScore. August 2014. http://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report