FireEye
SECURITY REIMAGINED

SPECIAL REPORT

OUT OF POCKET:
A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps

FEBRUARY 2015

CONTENTS

FEBRUARY 2015

EXECUTIVE SUMMARY

Mobile devices have become critical in today's digital workplace. But most organizations lack the security to ensure they, and the data they contain, are secure. Most security teams cannot fully account for—let alone monitor—the vast array of apps that have access to valuable corporate data.

Two main platforms dominate the mobile market today: Google's Android and Apple's iOS. FireEye researchers analyzed more than 7 million mobile apps on both platforms from January to October 2014.

WE FOUND THE FOLLOWING THREATS TO ANDROID DEVICES:

MALWARE

We found millions of mobile malware samples—and that number is growing by the week. Ninety-six percent of malware targets Android. KorBanker, which stole users' bank login credentials, is one example.

VULNERABILITIES

5 billion

More than five billion downloaded Android apps are vulnerable to remote attacks. One especially risky vulnerability is known as JavaScript-Binding-Over-HTTP (JBOH).

AGGRESSIVE ADWARE

5.61%

Aggressive ad libraries can leak personal data over the network— sometimes in plain text. Burstly is one of the most popular. It's used in more than 300,000 apps, including 5.61 percent of the 500 most-downloaded ones.

WE FOUND THE FOLLOWING THREATS TO IOS DEVICES:

VULNERABILITIES

UXSS

In particular, SSL/TLS misuse and other crypto-related vulnerabilities are common to apps. Attackers are also more often exploiting Universal Cross-Site Scripting (UXSS) vulnerabilities.

ENPUBLIC APPS

1400

These apps bypass Apple's strict review process by hijacking a process normally used to install custom enterprise apps. Many EnPublic apps invoke risky private APIs. In the wrong hands, these APIs threaten user privacy and introduce many vulnerabilities. We found only 1,400 EnPublic apps, a relatively low number. But this poses an intriguing avenue for attackers in the future.

MALWARE

Although uncommon, attackers are looking closely at this attack vector. They're eager to compromise devices that have not been "jailbroken." Attackers have started to use enterprise/ad-hoc provisioning to deliver iOS malware to non-jailbroken devices through trusted USB connections and over-the-air delivery.

INTRODUCTION

Mobile apps are fast becoming a hub of corporate activity, enabling workers to consume, create, and share information as never before. In 2014, mobile app usage accounted for 86 percent of time spent on mobile devices, up from 80 percent the year before.[1]

The right mobile apps can make a workforce more productive and nimble. The wrong ones can put its most valuable assets at risk.

Even as attackers find new ways to compromise this powerful tool, mobile security remains in its infancy. Most security teams cannot fully account for—let alone monitor—the vast array of apps that have access to valuable corporate data.

For enterprises with little insight into mobile security risks—and no way to deal with advanced attacks on mobile devices—apps represent a serious threat vector. Most enterprises lack control points to mitigate the risk of a malicious app coming into their environment.

Two main platforms rule the mobile market today: Google's Android and Apple's iOS. FireEye researchers analyzed more than 7 million mobile apps on both platforms from January to October 2014.

This report highlights the results of that review. We identify key threats to both mobile platforms, including vulnerabilities, targeted malware, and non-malicious apps with serious vulnerabilities. We also outline steps security leaders can take to make these devices more secure.

Mobile app usage accounts for 86% of time spent on mobile devices, up six percent in just one year.

Sarah Parez (TechCruch). "Mobile App Usage Increases In 2014, As Mobile Web Surfing Declines."

ANDROID THREATS

Android mobile devices combine sensitive personal data, photos, owner location and more with equally sensitive business data, contacts, and intellectual property. They also give those who want to steal it a new vector for attacks.

Our analysis of more than 7 million mobile apps during 2014 showed that mobile users face risks on many fronts including:

- Malicious apps that steal information
- Benign apps written in an insecure manner
- Benign apps that use insecure or aggressive ad libraries
- Malware and aggressive adware that are assumed safe because they pass Google Play checks
- Apps that enable attackers to steal users' identity
- Apps that profit attackers by calling for-fee phone numbers and texting services

ANDROID MALWARE SURGES

We've seen millions of samples of mobile malware, and that number is growing by the week. A vast majority—96 percent—target Android.

With Android, apps can pose as benign applications. Even some trusted, well-known apps include uncontrolled adware that gathers large amounts of user and device data for targeted ads.

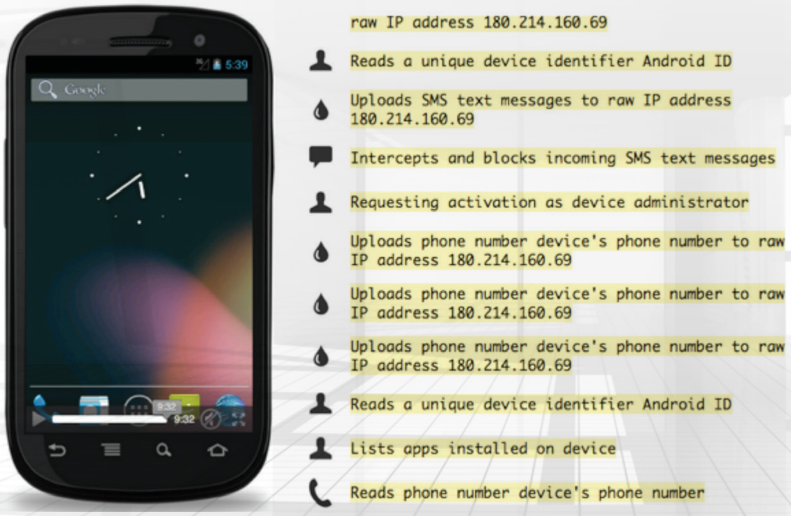
We found that Android malware (excluding adware and grayware) surged from roughly 240,000 unique samples in all of 2013, to more than 390,000 unique samples in the first three quarters of 2014.

One malware category of note: Android apps designed to steal financial data. The total rose nearly 500 percent in the second half of 2013. We saw more than 1,300 unique malware samples in December 2013, versus just 260 in June 2013.

WITH KORBANKER, BANK FRAUD GOES MOBILE

KorBanker is an especially nasty example of Android malware. It targeted several popular South Korean banking apps in 2014 to steal money. Disguised as a Google Play Store app, the KorBanker Trojan tricked the user into granting it device administrator permissions.

After users installed it, KorBanker used a fake login interface that resembled the user's banking app. Many people fell for the trick and provided their banking credentials. Those credentials were sent to attackers' servers in Hong Kong.



```
raw IP address 180.214.160.69
Reads a unique device identifier Android ID
Uploads SMS text messages to raw IP address
180.214.160.69
Intercepts and blocks incoming SMS text messages
Requesting activation as device administrator
Uploads phone number device's phone number to raw
IP address 180.214.160.69
Uploads phone number device's phone number to raw
IP address 180.214.160.69
Uploads phone number device's phone number to raw
IP address 180.214.160.69
Reads a unique device identifier Android ID
Lists apps installed on device
Reads phone number device's phone number
```

Figure 1. KorBanker app in action

BURSTLY

Burstly, now a subsidiary of Apple, runs an ad library platform that integrates third-party ad networks into both iOS and Android app platforms. Customers include Rovio, maker of the widely popular Angry Birds games.

Burstly collects detailed user information, such as:

- Age
- Number of children
- Education
- Ethnicity
- Gender
- Height
- Income
- Users' interests
- Location
- Marital status
- Sexual orientation
- Political affiliation
- ZIP code

Burstly collects this information over the life of the device, building an ever-more detailed profile of the user over time.

This profile enables the firm to sell highly targeted ads, which can earn publishers as much as five times more than non-targeted ads.

More than 300,000 apps use Burstly, including 5.61 percent of the 500 most-downloaded ones.

MANY ANDROID APPS VULNERABLE

More than 5 billion downloaded Android apps are vulnerable to remote attacks.

The Google Android platform has many vulnerabilities that attackers can exploit. The JavaScript-Binding-Over-HTTP (JBOH) vulnerability may be the riskiest.

A JavaScript binding method called addJavascriptInterface is a common way of loading web content into an Android app. It's also insecure. When an Android app invokes the method and loads the content from a web browser in WebView over HTTP, it opens the door for attackers to execute code remotely. (WebView is a way of showing web content in native Android apps).

In other words, attackers can hijack the HTTP traffic to inject malicious content and links into the WebView code—gaining full control of the app running on the device.

We reviewed popular apps (those with more than 50,000 downloads) to assess their exposure to the JBOH attack. Nearly a third, 31 percent, were vulnerable (see Figure 2). Of these JBOH-vulnerable apps, 18 percent fell into categories with potentially sensitive data: finance, medical, communication, shopping, health, and productivity.

Figure 2. The percentage of JBOH remote-exploitable app downloads on Google Play

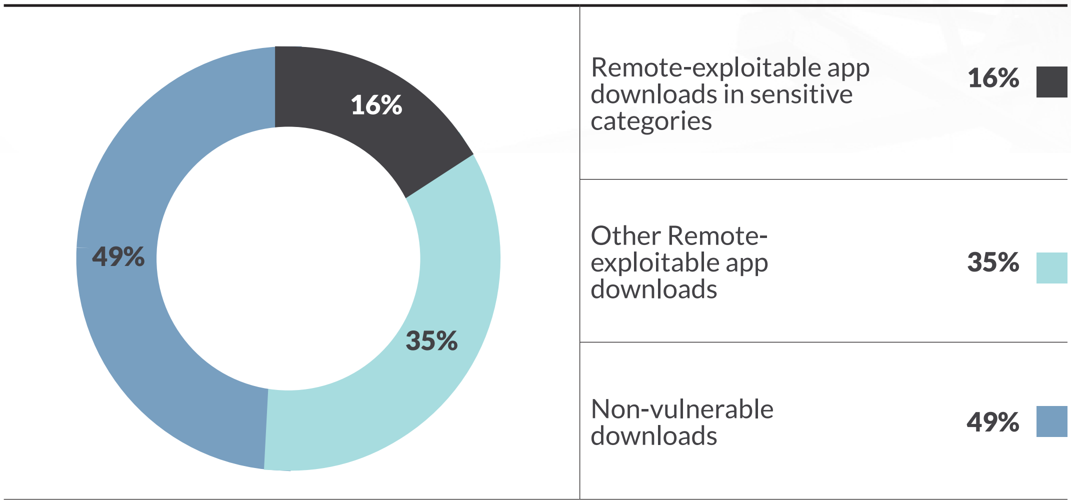
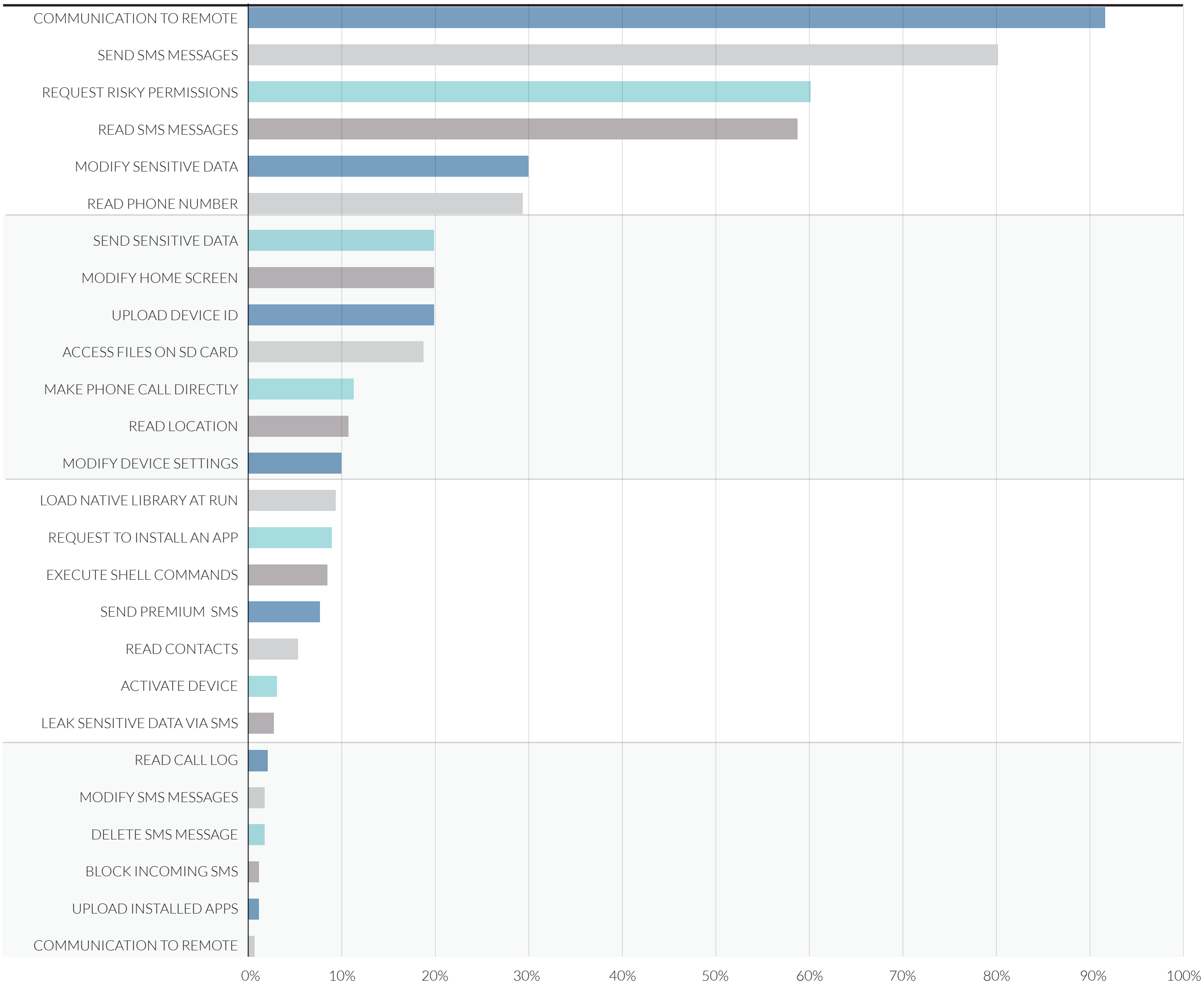


Figure 3: Percentages of observed mobile app behaviors



AGGRESSIVE ANDROID ADWARE

Aggressive ad libraries can leak personal data over the network—sometimes in plain text, easily readable to anyone who sees that traffic.

Adware is software that delivers ads to make money. While adware is not in itself harmful, it often aggressively collects personal information from the mobile device it's installed on: name, birth date, location, serial number, contacts, and browser bookmarks. Often, this data is collected without users' consent.

In our review, we examined ad libraries in Android apps. Adware is an increasingly popular option for app publishers, growing from almost 300,000 apps in 2013 to more than 410,000 in the first three quarters of 2014 alone. App categories that are the most likely to go the adware route include:

- Personalization apps
- Entertainment apps
- Lifestyle apps

App widgets, arcade-game apps, and communication apps are most likely to contain adware. That's because they contain rich information about a user's profile and interests, which makes them ideal for ad targeting.

Push-notification ads display ads as an Android's system notification. Many publishers of app widgets such as wallpaper and launcher apps have adopted this form of advertising because it captures users' attention—such ads require users to actively dismiss them—and limit ad displays to avoid annoying users.

iOS THREATS

iOS malware is still rare due to the strict review process of Apple's app store. But our analysis uncovered a new delivery channel for iOS malware that bypasses the review process completely.

We see a growing risk from enterprise apps not vetted by Apple's standard app review process. This exposes users to threats that would normally be blocked.

iOS threats can be classified into several broad categories:

- Vulnerabilities and information leaks, especially from background apps
- Public apps distributed through enterprise provisioning, also known as EnPublic apps
- Malware

iOS VULNERABILITIES: RARE BUT POTENTIALLY SERIOUS

In our review, we found that iOS vulnerabilities are infrequent. But their impacts can be severe.

For example, apps installed using enterprise/ad-hoc provisioning, and even some aggressive apps on the App Store, can exploit several iOS vulnerabilities.

In particular, SSL/TLS misuse and other cryptographic-related vulnerabilities are common to apps. Attackers are also more frequently exploiting Universal Cross-Site Scripting (UXSS) vulnerabilities.

> Attackers use undocumented APIs - which normally get an app rejected under Apple's review process - for powerful attacks.

UN-MASQUING A SERIOUS THREAT

The 2014 Masque attack had huge security impacts.

First, attackers mimicked the original app's login interface to steal the victim's login credentials. We confirmed this through multiple email and banking apps, where the malware uses a UI identical to the original app. The fake interface tricked the user into entering real login credentials, which were then uploaded to a remote server.

We also found that local data caches under the original app's directory remained in the malware local directory after the original app was replaced. The malware stole this sensitive data. We confirmed this attack with email apps where the malware stole local caches of important emails and uploaded them to remote servers.

Mobile-device management (MDM) technology cannot distinguish the malware-laden app from the original app because both use the same bundle identifier. No MDM API gets the certificate information for each app. Thus, it is difficult for MDM to detect such attacks.

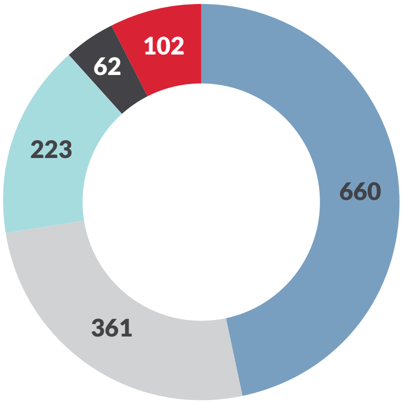
As mentioned in our Virus Bulletin 2014 paper "Apple without a Shell - iOS Under Targeted Attack," apps distributed using enterprise provisioning profiles (which we call "EnPublic apps") aren't subjected to Apple's review process.

As explained in the next section, that means attackers can use undocumented iOS APIs (which normally would get the app rejected in an App Store review) for powerful attacks. Attackers could, say, monitor users' actions. Or they could mimic iCloud's interface to steal the user's Apple ID and password.

The attacker can also use Masque attacks to bypass the normal app sandbox and get root privileges by attacking known iOS vulnerabilities, such as the ones used by the Pangu team to jailbreak iOS devices.

More than 80% of EnPublic apps use private APIs, which Apple prohibits.

Figure 4. Distribution of EnPublic apps



United States	**660**	🟦
China	**361**	⬜
England	**223**	🟩
France	**62**	⬛
Others	**102**	🟥

BYPASSING APPLE'S REVIEW WITH ENPUBLIC APPS

During our analysis, we witnessed a new delivery channel for iOS malware that bypasses the Apple App Store review process. We found more than 1,400 iOS apps freely available on the Internet, signed with enterprise certificates and distributed using enterprise provisioning profiles. We have named these EnPublic apps.[2]

Originally designed for building in-house apps, Apple's iOS Developer Enterprise Program has been abused to distribute iOS apps that aren't subject to Apple's review process. As a result, these published apps have none of the normal security and privacy controls.

More than 80 percent of the EnPublic apps were found to use private APIs, which Apple prohibits.

Figure 4 shows where these apps are distributed globally.

EnPublic apps can use private APIs within iOS and load user interfaces mimicking authentic Apple apps, which attackers use to attack iOS devices. Attackers can easily send victims a text message or email with a link to download an EnPublic app.

EnPublic apps represent a small volume of malware compared to Android. But this avenue of attack is likely to grow, and we will continue to monitor it. Wherever there is a way of bypassing Apple app store controls, iOS will appeal to all kinds of attackers.

NEW iOS MALWARE

Almost all of the iOS malware observed by FireEye works only against jailbroken devices. That changed in Autumn 2014 when two important iOS malware families were discovered and reported.

As predicted in our Virus Bulletin 2014 paper, both WireLurker and Pawn Storm abused enterprise and ad-hoc provisioning to install malware on non-jailbroken devices.

WireLurker used trusted USB connections to install malware onto both jailbroken and non-jailbroken iOS devices. On non-jailbroken devices, WireLurker also used enterprise provisioning to install the malware.

Unlike WireLurker, which was designed to take money from victims, Pawn Storm is espionage malware. It used ad-hoc provisioning to install on non-jailbroken devices. It collected sensitive data, audio, and screenshots and sent it to a remote Command and Control (C2) server.

[2] For more on EnPublic apps, see our 2014 Virus Bulletin paper: https://www.virusbtn.com/conference/vb2014/abstracts/WeiZhengXueSong.xml

CONCLUSION

People are adopting mobile devices across the world. PC sales are falling as consumers choose simpler, lighter devices that are easier to use. We spend more time on our mobile devices than watching TV, most of that time using apps. And users will likely continue to rely on apps for working, shopping, banking, socializing, and many other daily tasks.

For most users, mobile devices have become the most important tool they own. They contain our diaries, contacts, emails, photos, videos, employer details, and many other types of critical and sensitive information.

And yet mobile devices lack the security to ensure they, and the data they contain, are secure.

While mobile devices face many threats, app stores and app developers constitute the greatest risks. The apps we download, and their ensuing actions, have the potential to expose all information on the device.

Malicious apps can steal bank account details, copy emails, and collect VPN credentials. Adware can collect personal contact details, take note of all apps installed, and track GPS coordinates. And even in benign apps, developers make mistakes. They unwittingly write flawed code that leaves the app open to attack.

The major app stores are working hard to spot and reject harmful apps. But attackers will continue to stay ahead of security checks. Third-party app stores, while offering apps not available elsewhere, create a safe harbor for many more malicious apps.

App store providers, app developers, organizations, and users must better understand the threats and risks they face from mobile apps.

Consumers must pay special attention to app behaviors. Enterprises must consider mobile devices a key endpoint. And both sides must make understanding apps and securing them a priority.

For more about how FireEye can help identify and manage potentially harmful apps, please visit fireeye.com/products/mobile-threat-protection-mobile-security-products.html.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 3,100 customers across 67 countries, including over 200 of the Fortune 500.

[3] Simon Khalaf (Flurry). "Mobile to Television: We Interrupt this broadcast (Again)." November 2014.

To download this or other
FireEye Threat Intelligence reports,
visit: www.fireeye.com/reports

FireEye

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**