Q4 Mobile Security and Risk Review

October 1 - December 31, 2015

MobileIron

SECURITY LABS

Executive Summary

Welcome to the first edition of MobileIron Security Labs (MISL) quarterly Mobile Security and Risk Review. This report provides insights into the state of the mobile security and threat landscape, highlights emerging risks, and recommends ways to fortify mobile enterprise deployments.

Mobile device risks and threats are on the rise, and, as mobile becomes the predominant platform in the enterprise, we anticipate more mobile-specific vulnerabilities, malware, and network attacks. We see an increase in mobile device compromises, device vulnerabilities, and malicious apps. Furthermore, the attack surface is increasing due to increased risks.

Our research shows that more than 50% of enterprises have at least one non-compliant device at any given time. This is a direct result of users disabling PIN protection, losing a device, lacking up-to-date policies, and more. Non-compliant devices create a broader attack surface for malware, exploits, and data theft, and this heightened risk highlights the importance of using available security and compliance policies to quarantine non-compliant devices.

Our analysis also indicates that enterprises are still leveraging old security approaches to address next-generation mobile threats. A good example of this is the way in which enterprises are addressing cloud storage data loss risks. We found that enterprises are trying to address this risk by blacklisting one or more of the common cloud enterprise-file-and-sync-sharing (EFSS) apps. Blacklisting is like playing "whack-a-mole." With so many EFSS apps and services available, a blacklist policy will never catch them all, and users will just find another EFSS app to store their enterprise data in the cloud.

Furthermore, mobile malware and app risks continued to increase in 2015. In fact, new variants of malware, including YiSpecter and XcodeGhost, which target Apple's iOS, no longer require a jailbreak of the device. Yet we still see very low adoption of mobile anti-malware solutions such as App Reputation and Mobile Threat Prevention despite the fact that these solutions can mitigate the risks of mobile malware.

Finally, in the conclusion of this report, we outline next-generation security approaches to better fortify mobile enterprise deployments against malicious attacks.

The data in this report is normalized, anonymous data that has been collected from MobileIron customers. In subsequent editions of this report, we will continue to identify trends in this data from quarter to quarter. We believe that the data on which this report is based is the largest set of enterprise-specific mobile device security analytics across the three most popular mobile operating systems: Android, iOS, and Windows.

Mobile Threat Landscape

Despite 25 years of developing new security and defense techniques, PC and server breaches are at an all-time high. The highest number of breaches occurred in 2014; 2015 had nearly as many, falling short by just two breaches.[1] The good news is that mobile computing presents an opportunity to learn from the security mistakes of the PC era and to adopt a new security model.

With iOS, Apple introduced a sandboxed architecture to isolate data at the app level and protect both the file system and the operating system from unauthorized access. OS X, Android, and now Windows 10 have followed this model. As a result, all modern laptops and desktops will soon be running an operating system that looks like a mobile one.

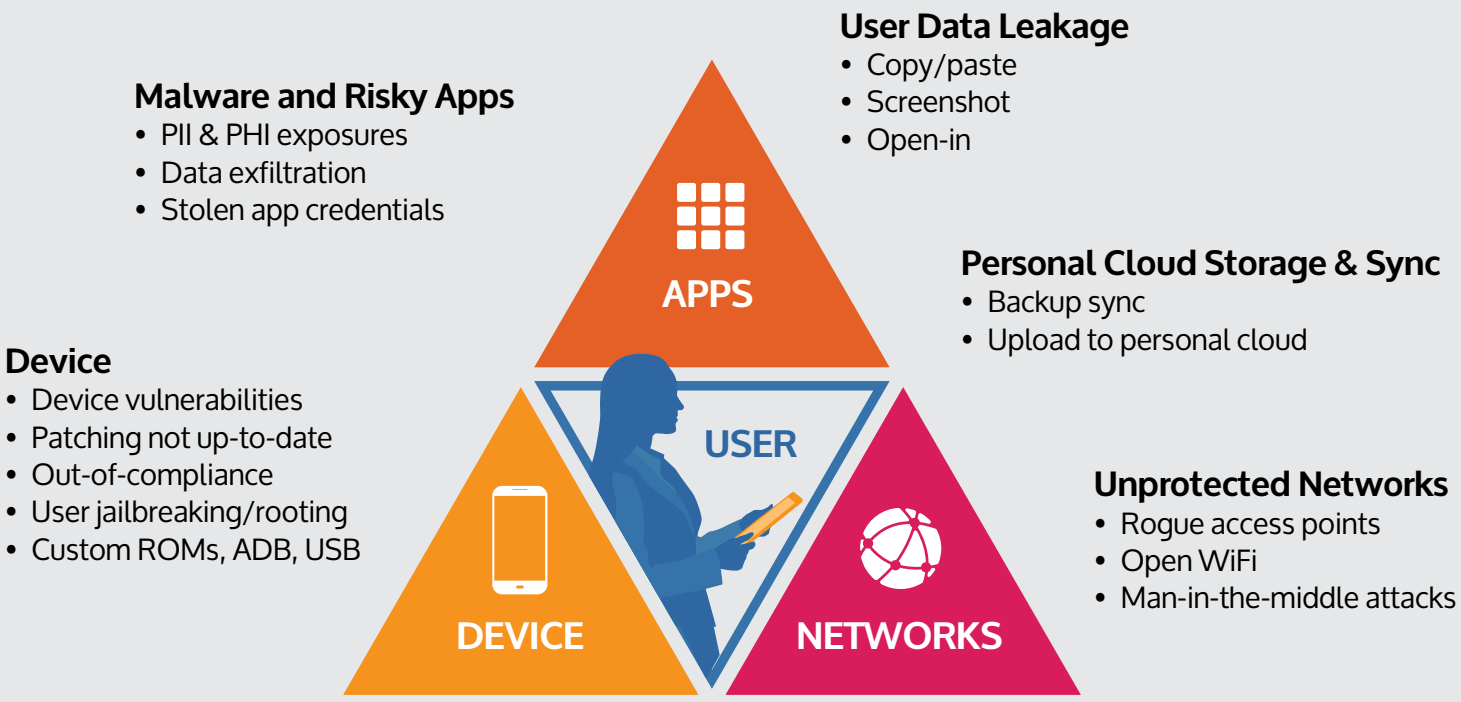
The mobile operating system architecture uses application sandboxing. This architecture is inherently more secure than the PC and Server architectures because, in mobile computing, operating system resources and data are isolated on an application basis. This is a fundamental shift from the traditional PC architecture, where systems resources and file access may be simultaneously shared across applications. Under the traditional PC operating system architecture, an attacker would distribute viruses, trojans, spyware, bots and other forms of malware through infected files that were introduced into the PC via malicious email attachment or downloads from an infected website. Once malware had gained a foothold on the PC, it was generally free to infect the operating system itself, thus impacting all apps and data on the PC.

In contrast to the PC operating system, application sandboxing under the mobile operating system architecture does not permit "cross-border" penetration of malware from one app to another or from one app to the operating system. Thus, the focus of an attacker has shifted from using a file to infect (and thus control) a PC to using an infected app to extract data based on user behavior or inherent vulnerabilities in the mobile device or network. This typically limits the attack surface to an app rather than the entire mobile device. But, as we note below, an infected app might still ultimately enable attackers to control the mobile device or gain access to personal information or important corporate data.

1 http://www.csoonline.com/article/3024797/security/data-breach-numbers-still-high-in-2015.html

Along with the change in mobile operating system architecture, there has been a fundamental change in user behavior. Mobile computing has been supported by an emergence of cloud and cloud-oriented apps that directly impact user behaviors. In the pre-cloud era, corporate data was generally maintained exclusively in access-controlled files behind a corporate firewall. In the post-cloud and post-social media era (a.k.a, the millennium era), however, end users rarely think twice about sharing personal or corporate data via cloud-based services. This poses a real challenge to enterprise administrators who must prevent and/or mitigate the risk of data leakage in order to protect trade secrets and comply with the various laws, regulations, and standards that apply to the handling of sensitive data.

MISL tracks ongoing and emerging threats across the mobile landscape. These threats are categorized by their method of attack through 1) the mobile device, 2) mobile apps, and 3) corporate networks (including cloud). The following diagram outlines these mobile threat vectors.



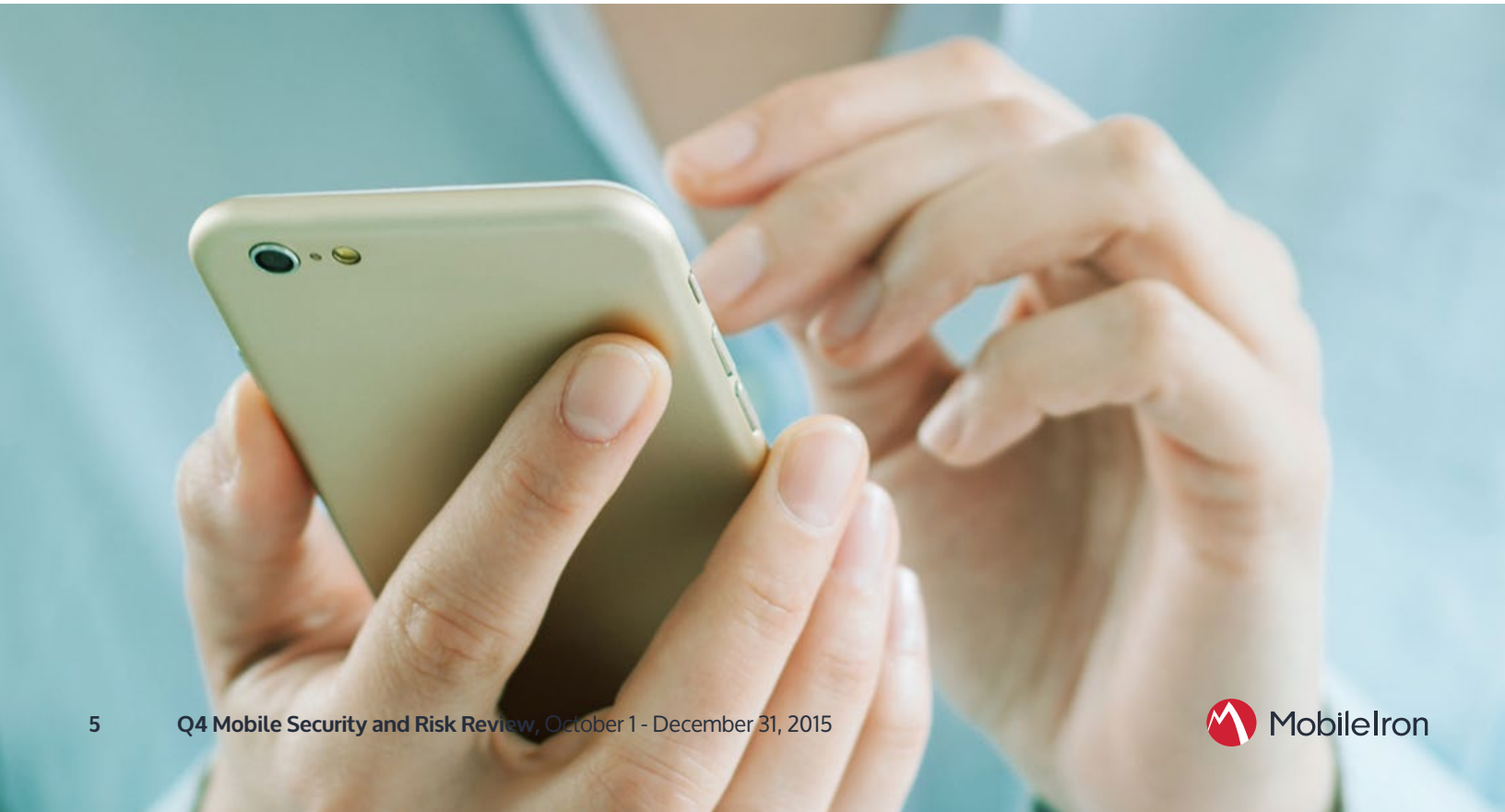
Mobile Threat Vectors

The security posture of devices can change over time due to a variety of factors. For example, new vulnerabilities in the operating system may be discovered, a user may jailbreak or root their device, or a user may disable their PIN, considering it to be a hassle. At the same time, mobile malware in the form of malicious apps, or even legitimate apps with risky behaviors, presents an increased risk of data harvesting or misappropriation of user credentials. In addition to these two threat vectors, networks outside of the enterprise's control can pose threats to data-in-motion when users travel and connect to open WiFi networks. Furthermore, cloud storage usage is at an all-time high. Dropbox is reporting that its users save 1.2 billion files to Dropbox every 24 hours. In addition, there are an increasing number of productivity apps for email and other uses that prompt users to upload data to third-party clouds as part of the normal course of app usage.

Old security approaches from the PC era underestimate these new mobile threats and overestimate traditional threats. The purpose of this report is to educate enterprises about new security approaches to these threats.

Operating System Trends: Android vs. iOS

Our data shows that iOS has 78% of the enterprise compared with 18% for Android. Please note, however, that the iOS/Android mix varies by region (for example, in Latin America, Android prevails over iOS). Readers should keep in mind that many of the enterprise risks identified in this report impact iOS and Windows deployments and are not limited to just Android. Therefore, they have a broad impact across all enterprise deployments and all three of these operating systems.



Device Risks

Until now, most companies focused their security concerns on Android vulnerabilities, risks, and malware because iOS was perceived as relatively invulnerable. That view is changing. For example, the National Vulnerability Database reported that in 2015 there were 375 Apple iOS vulnerabilities.[2] Anecdotally, industry press has reported on an increasing number of iOS malware variants including YiSpecter, KeyRaider, and XcodeGhost. It may be too early for any significant reporting on Windows 10 device vulnerabilities. Next-generation enterprise mobility management (EMM) solutions provide tools to identify and manage these device risks, as described in more detail below. These are broken out into device compromises, patching, and policy enforcement to maintain compliance with security policies.

Device Compromises

Last 90 days show the number of enterprises with compromised devices increased 42%

An EMM solution that enables the identification of compromised devices and triggers appropriate mitigation has become increasingly important in light of the increasing number of compromised devices. Our statistics show that as of December 2015, one in 10 enterprises have at least one compromised device. Furthermore, the trend from the first day of the quarter to the last day of the quarter, shows an upward trend, in which the number of enterprises with compromised devices increased 42%. In the absence of an EMM solution, a compromised device provides the attacker with an easily accessible platform to infiltrate a corporate network.

But what constitutes a compromise? Most enterprises have concerns about jailbroken (iOS) or rooted (Android) devices. For most, this is considered a binary function; it's either jailbroken/rooted or not. However, our security research has determined that device compromise is more complex than that. There are variants of jailbreaking tools as well as anti-detection tools that hide the fact that a device is jailbroken. This can create a false sense of security. A good EMM solution should be able to identify these variations of compromise and take appropriate action to minimize their effects.

Android is more complex than iOS due to the fragmentation stemming from vendors who create their own builds by customizing features. Some of these vendors employ custom ROMs (proprietary Android builds stored in Read-Only Memory) shipped directly from some manufacturers. This actually weakens the Android security controls and therefore presents a risk to the security posture of the device. In addition, there are device vulnerabilities that may allow privilege escalation (making data that is normally protected accessible), thus increasing the threat surface of the device. Furthermore, the Android Debug Bridge (ADB) can allow side-loading of apps, including unvetted apps that may have hidden malware or risky behaviors that may expose data. This is just a subset of the overall threats to Android devices.

2 http://venturebeat.com/2015/12/31/software-with-the-most-vulnerabilities-in-2015-mac-os-x-ios-and-flash/

Those enterprises who have not adopted an EMM solution have yet to understand the true impact that a compromised device may have on enterprise data. Most malware targets compromised devices, using the jailbroken or rooted device to gain unauthorized access to corporate network, data, and other resources. That is why an EMM solution is so important for protecting enterprise data from compromised devices.

Patching

The large increase in the number of iOS vulnerabilities stresses the importance of maintaining an up-to-date operating system that has resolved past vulnerabilities on the mobile device. Although this kind of patching tends to be user-driven, EMM policies can be used to enforce a minimum OS version and encourage users to upgrade and thus patch their devices. This is more difficult in Android due to the fragmentation, so policies like these are predominantly used in iOS. Our data analysis shows that, where an enterprise uses an EMM solution to enforce a minimum OS version, users tend to run iOS versions that are relatively current. Although most EMM solutions can enforce OS upgrades, our research shows that less than 10% of enterprises are using this enforcement policy.

Less than 10% of enterprises are enforcing device patching

Policy Enforcement

An enterprise must be able to enforce policies designed to protect the integrity and security of data-at-rest and data-in-motion. Such protection is critical to preserving the confidentiality of employee personal data as well as corporate trade secrets. It is also a fundamental requirement for most regulatory compliance such as PCI and HIPAA. In analyzing the data, we noted that 53% of enterprises had at least one device that was non-compliant with at least one of the policies described below. MobileIron's solution gives enterprise administrators the ability to identify devices that are non-compliant and to take appropriate remedial action (e.g., quarantine, selective wipe, etc.) against those devices.

Our analysis identified some interesting non-compliance trends with enterprise-managed mobile devices:

33%
had missing devices
Out of contact for an extended time (Missing device that may be lost or stolen)

22%
had users remove PIN
Disabled PIN or passcode enforcement

5%
had users remove MDM
Removal of mobile device management (MDM) App

20%
had devices with old policies
Out of date devices occur when the mobile IT administrator has changed a policy on the console but that change has not propagated to all devices

App Risks

Ninety-six percent of mobile malware variants target Android[3] but, as noted earlier in this report, 2015 saw a significant rise in iOS malware. More alarmingly, some new iOS malware no longer requires that the device be jailbroken. Malware such as XcodeGhost exploited Apple's Xcode SDK, which is used by developers to create iOS apps, and circumvented Apple's App Store security review processes. This allowed users to unknowingly download malicious apps from Apple's curated App Store. FireEye identified more than 4,000 apps in the App Store infected with XcodeGhost.[4] While Android continues to have the largest volume of malware, in 2015 it became clear that iOS is no longer impervious to threats.

3 http://www.bbc.com/news/technology-35070853
4 https://www.fireeye.com/blog/executive-perspective/2015/09/protecting_our_custo.html

Less than 5% of enterprises have deployed a mobile anti-malware solution

MobileIron relies on its ecosystem of partners to allow an enterprise to choose an App Reputation or Mobile Threat Prevention solution for identifying mobile malware. These detections are integrated with MobileIron to allow MobileIron to take action by quarantining the device. Despite the benefits and ready availability of these solutions, our research shows that less than 5% of enterprises have deployed an App Reputation or Mobile Threat Prevention solution to-date. Considering that 2015 was a breakout year for iOS malware and vulnerabilities, we expect App Reputation and Mobile Threat Prevention adoption to increase in 2016. It is also now appearing in some regulatory and industry compliance mobile requirements, which should further drive adoption.

These App Reputation and Mobile Threat Prevention vendors can identify malicious apps, risky apps, network attacks, device vulnerabilities, and more. We strongly recommend that this type of solution be deployed as an additional layer of defense.

Network Risks

Mobile data loss can occur from a variety of threat vectors, but one of the most prominent risks today is data loss from files being saved in cloud storage services or Enterprise File and Sync Sharing services (EFSS). Many organizations are still trying to determine how to best protect against this risk. In addition, users also have access to built-in features such as iCloud and Google sync services which are part of the native experience on their devices. With so many options available to users, the cloud risk landscape continues to grow. What this means to the enterprise is that employees may be, willingly or unknowingly, putting sensitive corporate

MobileIron

data at risk of loss. Such loss can occur from unauthorized access to the cloud-based files in which the data may be stored or from intentional leakage to unauthorized persons. In any event, absent the data monitoring and cloud access control features of a modern EMM solution, the enterprise has little visibility or control over data leakage via cloud services.

One unsophisticated and outdated method for trying to manage data leakage via the cloud is "blacklisting." Blacklisting is a policy within a mobile application management system that allows a device to be quarantined, selectively wiped, or blocked when a blacklisted app is detected. In the early days of mobility, blacklisting was a standard approach used to block unwanted apps in the enterprise. These policies were traditionally manually created by the administrator but are simply not scalable with the enormous number of mobile apps available today.

More importantly, in many cases, such outdated tools and policies fail to distinguish cloud services apps that are designed to enable enterprise data migration control (e.g., via managed "open-in" features or enhanced user authentication) from "consumer" apps.

More recent versions of EMM solutions (such as MobileIron) use the managed application/containerized approach to enable administrators to blacklist the unauthorized (consumer) version of cloud apps while allowing the managed (enterprise) version of such apps. As our data shows, five of the top 10 blacklisted apps are consumer versions of an EFSS app.

The top 10 consumer apps most often blacklisted by enterprises are:

1. Dropbox (consumer version)
2. Angry Birds
3. Facebook
4. Microsoft OneDrive (consumer version)
5. Google Drive (consumer version)
6. Box (consumer version)
7. Whatsapp
8. Twitter
9. Skype
10. SugarSync (consumer version)

Thus, a "next-generation" EMM solution allows the administrator to permit an enterprise-approved cloud sharing app, such as Dropbox for Business or Box for EMM, while blocking unauthorized consumer apps from storing enterprise data in the cloud. Identity protection and cloud access control solutions now provide additional layers of protection to mitigate data loss.

Summary

For most enterprises, mobile security strategies are still maturing. Analytics based on the prevalence of identifiable vulnerabilities in mobile devices, apps, networks, and user behavior are key to developing better tactics and tools to reduce the impact of these vulnerabilities. Enterprises with an EMM solution in place generally have many of the tools they need; they just need to activate them.

Recommendations

Enforce compliance policies and quarantine devices that fall out-of-compliance. Because a non-compliant device is a prime target for a malicious attack on the enterprise, we strongly recommend aggressive use of strict compliance policies with an EMM solution to quarantine non-compliant devices. The EMM solution can detect a user who has disabled their PIN, compromised the device, has an out of date policy, and more. Quarantine features can be used to block network access and/or selectively wipe the corporate data from the device. This mitigates data loss, supports regulatory compliance requirements, and avoids being the next headline.

Give up on blacklisting personal cloud storage apps and, instead, leverage EMM-provided, managed app solutions or containerization to provide a secure enterprise cloud storage solution to your employees. The EMM approach, which is based on blocking the dissemination of enterprise data rather than blocking an ever-increasing number of cloud apps, has the further benefit of keeping enterprise data separate from personal data.

Add an App Reputation or Mobile Threat Prevention solution that integrates with your EMM solution. These solutions will detect malicious apps, malware, app risks, network attacks, and more. And they all leverage the EMM solution to take action and quarantine the device when a threat is detected.

Enforce patching of your managed devices. This can be done through the EMM console by enforcing a minimum operating system version. This is simple to do for iOS, but becomes more complex with Android due to the fragmentation described earlier. However, the previously mentioned App Reputation and Mobile Threat Prevention solutions can identify Android device risks by correlating known vulnerabilities against the Android operating system. These solutions can then notify the EMM solution when a vulnerable device has been detected so the device can be quarantined.

Automatically quarantine compromised devices even if the device is "offline." The native functionality in an EMM solution allows an enterprise to identify a jailbroken or rooted device and quarantine it automatically even if the device is not connected to the network. This is a major advantage over solutions like native ActiveSync which has no visibility into compromised devices.

The advent of mobile computing requires enterprises to build a new security approach, and intelligence is essential to be able to make educated decisions about cyber security defenses. In *Leadership Lessons of the Navy Seals*, authors Jeff Cannon and Lt. Commander Jon Cannon share the following, which holds true for cyber security too:

> *"No single structure is ideal for all missions. Without continual and intelligent modification, they will work only in the best of circumstances and fall apart when the situation changes."*

This report is intended to provide that necessary intelligence through analysis, insights, and recommendations that will help enterprises define and refine their next-generation mobile security strategy. At MobileIron Security Labs, we look forward to delivering new intelligence next quarter.

MobileIron

SECURITY LABS