wandera

The Evolution and Impact of Hidden Mobile Threats

Protecting your organization from risks

Table of Contents

Executive Summary

The explosion of billions of mobile devices has created the largest technology footprint for hackers to steal corporate and personal information.

The basic protections provided by mobile operating systems do not eliminate the risk of external threats, but they have significantly changed the conversation around security. Some of the most widely utilized mobile platforms today are perceived to be secure. This had led to an industry that has become distracted by focusing on an antiquated definition of "threat". Advanced anti-malware solutions, VPNs and firewall appliances will not protect a mobile workforce when the users are actually mobile. To be successful at building a truly secure mobile ecosystem, the industry needs to take a new look at the real problems posed by mobile computing.

The history of technology is that every system created is eventually compromised. The unique position of mobile devices is that they serve as both a business tool and a personal one. Companies with employees that use mobile devices, whether corporate or personally owned, have to understand the security threat these devices pose to corporate information, but also understand the access rights that these devices require.

This whitepaper explores the types of threats attacking mobile devices and suggests an innovative approach for organizations to adopt in preventing these threats from stealing valuable personal and corporate information.

Introduction

Attacks on mobile devices, which were rare only a few years ago, are increasing, and are, in many ways, different from those in a desktop computer world. Breaking news about new mobile threats is common place and will only become more prevalent. The mobile threat landscape has unique characteristics that complicate the challenge facing mobile security professionals:

There are six main reasons for the increase in attacks:

1. **Large attack surface** - The explosive growth of the market for mobile devices. With billions of devices now in users' hands, this demand has created the largest technology footprint for hackers to steal corporate and personal information.

2. **Unprotected technology** – Today, the reality is that these devices are typically unprotected. With virtually nothing protecting mobile devices, there is no barrier to prevent hackers from attacking with impunity. With no chance of being caught, there is no deterrent to the potential cyber criminal.

3. **Access to corporate networks** - Insecure mobile devices are exploitable to gain access into corporate networks. Because mobile devices contain a hybrid of both personal and corporate information, they are increasingly targeted by cyber criminals.

4. **Financial incentives** – Maybe the most important is that, by compromising the mobile device itself, the rewards are lucrative for cyber criminals.

5. **Risky user behavior** - Whether it's the effect of Apple's walled-garden approach, or the relative nascence of the mobile threat landscape, end users have a false sense of security when it comes to their mobile devices. Unsuspecting end users can grant apps widespread permissions and even provide root-level access by jailbreaking their phone, whilst relying on their device for sensitive tasks such as online banking. Employers need to educate their employees on these threats and provide best practices to prevent mobile attacks. A recent poll of over 2,000 end users, conducted by Wandera, uncovered that only 7% of employees have been given any form of security guidance on using apps and smartphones in general.

6. **Hybrid device for both business and personal use** – 70%[4] of employees access corporate data from a personal smartphone or tablet. The security challenge of protecting corporate data is not limited to BYOD devices. Employees are using corporate-owned devices for personal use and want control over the device.

Your organization has likely already suffered from multiple instances of data theft, intercepting requests or gaining control over individual mobile devices.

It is also likely that IT Administrators in your organization are unaware of such attacks. Individually each attack may not result in large financial and public relations costs, making them harder to detect and perhaps a lower priority to address. However, cumulatively they bear significant financial cost to your organization, and make it susceptible to further organized attacks in the future. Detecting and remediating these hidden mobile threats should be a priority for your organization.

The environment surrounding mobile devices is going through a rapid evolution and threats are gaining in sophistication and the danger they pose to users is increasing.

Mobile Threat Types

First, you must consider the nature of the security threat that is attacking the mobile device. There are three types of people threatening the mobile device.

Person	Description of Threat	Potential Solutions
The Insider	Uses the company device. Steals data from the company by copying it to another cloud storage service. Copies valuable corporate content from email.	Mobile Device Management (MDM) and App Containers
Common thief (non-cyber)	Stealing the device to re-sell, not typically interested in the data on the device. If a device is stolen or lost, the security imperative is to wipe the device of any corporate information.	Mobile Device Management (MDM)
Outside cyber attacker	Sophisticated hacker compromising the device to gain access to information on the device or access the corporate network.	Wandera Data Security and Management

To understand the sophistication of mobile threats, it is helpful to also categorize them by what technology is involved. There are four broad threat categories in the mobile ecosystem.

Device Threats

The device itself is under attack. It may seem obvious, but basic mobile device configuration is often overlooked because people assume that the core mobile operating system is secure. The reality is that device configuration matters. A corrupt, tampered or altered configuration can make the device vulnerable. Configuration threats include Jailbreaks, Outdated Operating Systems, Semi Jailbreaks and Malicious Profiles.

App Threats

Interestingly, the 'app store' model has given people a false sense of safety with the impression that an app is safe if it passed the review criteria and gained admission. The truth is that the review process suffers from security flaws. With millions of apps in App Store environments, and more being created everyday, the rush from developers is to create features to make a sticky and popular app. They are not focused on security. On top of that, App Store owners primarily review the app for usability and design specs rather than worrying if personal information is vulnerable.

The XcodeGhost Malware infection was a direct attack on the trust given to the App Store. This attack compromised the Apple App Store policies and was one of the most serious mobile attacks to date. It placed malware in one of the building blocks of code used by developers to build apps. Hundreds of apps used by millions of users were created with malware inside.

Think about all the apps on your phone. The vast majority will communicate at some point to web services. It could be a game sending high scores, photos performing backups or third parties connecting to display advertising content. If a hacker is able to open up the web services, and you've given an app permission to access your personal information, you're opening up that vector to the attacker. Insecure App threats include Leaks, Ad Servers, Sideloading and Permissions.

Infrastructure Threats

With the proliferation of mobile devices, the growth of Wi-Fi hotspots has skyrocketed. And as an attack vector, these rogue hotspots are the perfect vehicle to intercept a user's traffic. Infrastructure threats include Rogue/Malicious hotspots, Man in the Middle attacks and Certificate spoofing.

Network and Web-based Threats

Distribution of these attacks is the same, regardless of whether they are accessed from a desktop machine or a mobile device. Malware can be accessed from a browser and brought onto the device by the user. Spam and phishing are also prevalent because users have both personal and business information and apps on devices and can unsuspectingly click on a link in email or text message and access malicious content.

Mobile Threats Explained

OS

DEVICE THREAT

Outdated OS

In the cat and mouse game of OS vendor patching of known vulnerabilities whilst hackers race to exploit them, a device running an outdated OS is by definition vulnerable and presents a significant risk of being compromised.

There are more than 11,000 different combinations of Android devices[7] and Android Operating Systems in existence. This fragmentation creates a management headache and a security issue whereby many devices remain with outdated OSs. This is also a challenge on the iOS platform. Evidence suggests that 24% of iPhone users were on an older OS, even 5 months after the release of the new iOS[8].

In an enterprise setting, IT departments sometimes choose to implement a phased approach to OS upgrades for their mobile device fleets to keep in step with releases to their MDMs and this staggered approach also creates devices with outdated OSs.

DEVICE THREAT

Jailbreaking

It is never safe to have a jailbroken device in your corporate network. Jailbreaking, or rooting, is the process of removing the security limitations imposed by the Operating System vendor. Jailbreaking permits root access to the OS file system allowing the download of applications which are not permitted through the official app stores. Jailbreaking also provides all apps, including malicious ones, with access to data owned by other applications.

End users often jailbreak a device in order to gain access to a capability or app that is not officially supported, or to unlock their phone so that it can be used with other carriers. It is possible that the employee may not even know that their device has been jailbroken.

APP THREAT

Vulnerable Legitimate Apps

Mobile users face significant threats from legitimate apps that are downloaded from official app stores.

Over 75% of the top iOS and Android apps have permissions to access user data. Poor programming often results in apps inadvertently leaking this sensitive user information. They do this by passing plain-text data in transport or storing data on the device without the necessary security measures. Gartner has predicted that by 2017, 75% of mobile security breaches will be the result of mobile application misconfigurations. Since advertising is a primary source of revenue for most free and even paid apps, data is also often shared with ad networks.

As a recent example, the security team at Wandera discovered a serious security hole in the popular NFL Mobile app just days before the big game between the New England Patriots and Seattle Seahawks. The vulnerability was leaving highly valuable personal information exposed to man-in-the-middle (MiTM) hacker attacks.

Similarly, research done in January 2014 by IO Active Labs discovered that, of the 40 home banking apps from the top banks in the world, 20% were vulnerable to man-in-the-middle attacks and 40% leaked sensitive information like activation codes through plain-text requests, or exposing data through the device logs. These results were surprising given the size and resources of the financial institutions and the focus from cyber criminals on mobile banking malware.

APP THREAT

Malicious Apps

Mobile malware is malicious software designed to steal personal information stored on the device or gain control over the device. Most mobile malware spreads via malicious apps that persist on the device and gain extensive permissions.

Google's Android platform is most vulnerable to malware due to the level of control the platform provides developers and the ability to download apps from 3rd party stores that are not vetted by Google.

However, the iOS platform is not completely worry-free either. For example, a flaw found recently in Apple's iOS allowed hackers to intercept email and other communications that were meant to be encrypted. Other techniques that hackers employ on the iOS platform are malicious profiles or rogue certificates. A malicious profile can overwrite system functionality such as MDM software or mobile carrier settings, and be used to bypass various security measures and potentially intercept all data packets. Hackers can also gain access to a developer certificate or enterprise certificate, allowing a malicious app to be installed directly without going through Apple's app store. Finally, as discussed earlier, a jailbroken iOS device removes all the security limitations imposed by Apple making it extremely vulnerable to malware attacks.

The top categories in mobile malware include:

- **Premium Service Abuser** – Sends text messages to premium mobile phone numbers, racking up unauthorized charges.
- **Information Theft** – Similar to adware and some legitimate apps, this type of malware leaks sensitive information. The intent is almost always to find sensitive information that can be sold or exploited for other attacks such as phishing or mobile banking fraud.
- **Malicious Downloader** – Downloads malicious apps and files, its main objective is to download more malware. Numerous malicious apps contain multiple types of threats and mechanisms for spreading. As an example, a Trojan named Obad sends messages to premium rate numbers, downloads and installs other malware, and uses Bluetooth to install itself on other devices.

INFRASTRUCTURE THREAT

Compromised Wi-Fi Hotspots

With over 5.8 million hotspots expected by the end of 2015[9], free Wi-Fi has become ubiquitous and convenient, but also a prime target for exploitation.

The attacker may create a spoofed Wi-Fi network (e.g. 'Free-Starbucks') or simply connect to the same legitimate Wi-Fi that the victim is using with tools like Droidsheep. Either way, all communications end up passing through the attacker-controlled network device. They can easily intercept passwords, credit card details and other sensitive information that can lead to identity theft, financial compromises or access to your corporate network.

Even websites with SSL encryption are not bulletproof. Hackers can modify the encrypted (SSL) network's communication by using spoofed certificates, or by downgrading the communication link, so that it's un-encrypted and completely open to the attacker. In these scenarios any data such as email passwords, banking details and other valuable information can be intercepted and stolen.

In a recent poll conducted by Ofcom, it was discovered that 55% of adults used the same password for most web services. This is an important aspect of user behavior. Even if hackers exploit just a single innocuous site or app, it will provide them with access to multiple other high value assets.

NETWORK & WEB THREAT

Phishing

Phishing is one of the oldest means of Internet attack. Authentic-looking emails or websites are presented on the device, and vulnerable users are deceived into volunteering sensitive information such as their as username, password and credit number to the hackers.

Smartphone users are three times more likely to share their various account login and password credentials on malicious phishing sites[10]. This is due to the fact that users are constantly checking email accounts on their mobile device, often multi-tasking and so not paying full attention. Furthermore, the mobile device screen real estate is too small for users to accurately determine the legitimacy of a URL.

On mobile, phishing attempts can be delivered over SMS as well as email. In addition to fake websites, employees are also being targeted by apps designed to impersonate popular apps.

A type of phishing attack known as spear-phishing targets specific organizations to gain unauthorized access to confidential data, rather than a generic phishing attempt to large group of people. The larger the organization, the greater the risk of a spear-phishing attack. One in 2.3 companies with over 2,500 employees were targeted in at least one spear-phishing attempt, whereas one in five small or medium businesses were targeted[11].

Threat Correlation of the Risky User

Unlike the PC platform, mobile threats are highly correlated. A user with an infected device is more likely to suffer from other mobile attacks. This is often because:

- Users who grant widespread permission to legitimate apps are most likely to download malicious apps.
- Malicious apps generally exhibit multiple bad behaviors and are designed to spread to other devices by gaining access to the address book.
- Jailbroken phones are more susceptible to malware.
- A device with malware is most at risk of being exploited if there is a password or data leak by a legitimate app.
- A user whose device leaks information like an email address is an easy target for phishing.

Risky users carry risky devices. And understanding the usage of risky users is a good way to limit exposure for an organization. Detecting and remediating these mobile threats should be a priority for your organization. The compounding effect of mobile threats further stresses the need to proactively address these vulnerabilities before they reach an inflection point where impact and cost start to snowball.

Potential Security Solutions

Now that we have detailed the threats to businesses when it comes to mobile security, let's discuss possible solutions. Several fragmented security solutions exist to address the different mobile threats that enterprises face today.

MOBILE DEVICE MANAGEMENT (MDM)

MDM solutions offer some valuable security features focused on the device. The use of containers around email or other business apps preventing data being copied from container to elsewhere is a solution to preventing the malicious insider stealing corporate secrets. But the best security feature is the ability to remotely wipe a lost or stolen device. This solution is really aimed at protecting enterprises from the inside threat who loses their phone or the common thief who stole the device. The configuration of the device at deployment is set to adhere to company policies and there are periodic checks to confirm which apps are loaded on the device, but once the device is in the hands of the user, and between these checks, the MDM doesn't have real-time visibility into how it is being used. Most importantly, the MDM service has no view into what is happening to the data going into, and out of, the device. Therefore, it is of no use to protect against a cyber hacker attacking the device from the outside world.

APP REPUTATION SERVICES

App reputation services provide information on the risks associated with apps on your employees' devices. However, with the constantly changing landscape of both mobile threats and the frequent updating of legitimate apps, a list-based approach has limitations in detecting the latest threats. Similarly, antivirus (AV) solutions and malware scanners are reactive to the latest attacks and cannot adapt to the changing and interconnected threat landscape.

APP WRAPPERS (AND ENTERPRISE APP STORES)

App wrappers and enterprise app stores adopt a whitelist approach allowing employees to only download pre-approved apps. These 'locked-down' solutions are typically not feasible for BYOD devices. Employees also expect more control over corporate-owned devices and a whitelist approach can result in a negative experience. On average, smartphone users are downloading 15 apps each quarter. Not all apps are compatible with these approaches and it's inefficient to maintain lists that require IT managers to decide what apps to approve and go through manual steps to add and remove those apps.

SECURE APP CONTAINERS

Secure containers that provide full auditing and true single sign-on (SSO) are quite effective in protecting some corporate data, but do not provide any protection outside of the container and typically also result in a negative user experience.

WEB SECURITY

Cloud proxy services protect users from malicious sites on the internet. From blocking access to known malware, phishing or spam servers, they are effective at protecting organizations from outside threats. However, most are built for PC-based threats and not built focused on mobile devices. This focus on legacy PC techniques lead to blindness when looking at all the data going through a mobile device.

With weaknesses evident in current solutions, the most effective security solutions today should address first, the main groups of people that are creating the security problems, the malicious insider threat, the common device thief and the outside cyber attacker, and also take into account the technology used, and prevent threats attacking the device, the apps, the infrastructure and those living on the web.

A Comprehensive Mobile Data Security and Management Solution

Fortunately, Wandera was built with a mobile-first philosophy. It was built for mobile devices from the ground up.

Wandera offers protection against a full spectrum of mobile threats. Our unique multi-level architecture, both on device and in the cloud, creates the largest mobile dataset of information in the industry, provides enterprises, in real-time, with:

- Unrivaled visibility into their mobile data
- Cloud analysis of the risks within the data
- Powerful policy controls to prevent security threats, ensure compliance and manage usage

Because Wandera lives on device and in the cloud, we are unique in that we see all the data going into and out of the device.

How Wandera Works

UNDERSTAND USAGE WITH THE WANDERA MOBILE APP

The starting point for Wandera is our lightweight app on the device. The Wandera Mobile App is employee-friendly and helps educate users on their data usage and notifies them of any important policy updates you've introduced. Most importantly, we alert them directly for any major security event.

The App monitors the pulse of the user device, whether smartphone or tablet, and collects these Heartbeats for analysis. It's the first, but important, view into mobile data. For example, Wandera can identify connections to rogue infrastructure like malicious Wi-Fi spots.

BETTER DATA VISIBILITY WITH WANDERA'S CLOUD GATEWAY

Mobile devices today are impressive but cannot compare with the computing power available from the cloud. Our cloud gateway is what gives you the real-time view into your mobile data. With increased visibility comes increased knowledge about threats. By sitting transparently in the path of the web traffic from the browser to mobile applications, we analyze mobile data usage as it happens, immediately detect threats, and enable in-line policy actions. And all with no impact on the user experience.

CLOUD INTELLIGENCE FROM SMARTWIRE

The billions of daily mobile data inputs collected through our multi-level architecture are analyzed in real time by SmartWire, our cloud intelligence engine.

SmartWire utilizes non-signature detection techniques and automated machine learning to dynamically generate fine-grained heuristic parameters that build up a detailed view of each mobile data request and the associated security risk.

The network effect of knowledge is used to prevent threats from billions of data points.

Mobile Threat Coverage by Security Solution Type

Threats	Wandera	Mobile Device Management (MDM)	App Reputation	App Containers	Endpoint Protection	Web Security
Real-Time	Yes	No	No	No	No	No
Architecture	Multi-level. On device and in cloud.	Single-level. On device only.	Single-level. On device only. Requires MDM.	Single-level. On device only.	Single-level. On device only.	Single-level. In cloud only.
Type of Threat	Outside Threat	Inside Threat and Theft of device	Outside Threat	Inside Threat	Outside Threat	Outside Threat
Device Threats	✓	✓			✓	
Jailbreak	✓	✓			✓	
Semi Jailbreak	✓					
Outdated OS	✓	✓			✓	
Malicious profiles	✓	✓			✓	
Application Threats	✓		✓	✓		
Approved Apps leak PII	✓			✓		
Ad servers, Third Party API's	✓		✓	✓		
Side-loaded Apps	✓		✓	✓		
Apps with inappropriate permissions (Calc using Location, etc,	✓		✓	✓	✓	
Infrastructure Threats	✓				✓	
Rogue/Malicious Hotspots	✓					
Man in the Middle Attacks	✓				✓	
Certicicate Spoofing	✓					
Wi-Fi Phishing attach	✓					
Network & Web Threats	✓					✓
Malicious websites/ apps	✓					✓
Browser exploits	✓					✓
Phishing servers	✓					✓
Spam servers	✓					✓

Conclusion

Mobile threats are here to stay. The impact of new mobile device attacks will continue to grow. The types of threats are wide and varied but many are aiming their sights on the mobile ecosystem. It may be the largest footprint of devices technology has seen.

Your organization faces a real risk from hackers stealing data or gaining control over employee mobile devices. Preventing these attacks should be a top priority, however we can see they present a unique set of challenges.

Security solutions are looking at many areas to offer protection. But some solutions are providing a wider coverage for the full spectrum of mobile threats.

Wandera's Mobile Data Security and Management solution is a strong solution to consider when protecting an enterprise's mobile data.

About Wandera

Wandera is the leader in mobile data security and management, providing enterprises with unrivalled visibility into their mobile data, and protecting them with real-time threat prevention, compliance and data cost management.

WANDERA US | 180 SANSOME STREET, SAN FRANCISCO, CA 94104 T +1 (415) 935 3095 INFO@WANDERA.COM
WANDERA EMEA | 45 MORTIMER STREET, LONDON, W1W 8HJ T +44 (0) 203 301 2660 WWW.WANDERA.COM