Table of Contents

3 Introduction

4 Testing Methodology for this Report

5 Enterprise Mobile OS breakdown

8 ‘Dead Apps’ are the biggest risk to the Enterprise.

10 Global Look at Mobile Threats
Introduction

Mobile devices have fundamentally changed the way businesses conduct themselves. The promise of unleashing productivity by untethering the workforce has driven adoption of new technologies such as smartphones and tablets across Enterprises globally. But the security concerns BYOD and corporate-owned devices bring along with it cannot be ignored. The introduction of such devices, and the apps they carry into the workplace, often precedes the ability to test and secure them. As a result, mobile devices and mobile apps present unique technological, legal, and security challenges for IT and Security professionals.

The risks arise from liabilities involved in granting access to sensitive personal or financial information, or exposing corporate assets such as intellectual property or confidential information that could be breached. Gartner predicts that by 2017 the majority of malware authors will have turned from PC endpoints to mobile devices. Enterprises have to dramatically shift their way of thinking to simultaneously encourage and embrace the influx of mobile devices, and more importantly, mobile apps, into the workplace while meeting internal and regulatory security requirements.

Appthority’s Enterprise Mobile Threat Team (EMTT) was created to monitor and research the latest mobile risks that are direct threats to the enterprise. The purpose is to help organizations holistically assess and protect their people, data, applications, and networks from risks and exposures in the mobile threat landscape. The EMTT is composed of security industry veterans that have decades of experience in protecting mobile devices.

We are proud to present our first quarterly edition of the Enterprise Mobile Threat Report that explores the current challenges faced in mobile security. We review the new challenges and risks that Enterprises face that accompany paradigm changes such as Dead Apps, the latest trends in mobile malware and other issues related to securing mobile devices—and your Enterprise. We invite you to follow our latest findings on our blog: www.appthority.com/enterprise-mobile-threats
Testing Methodology for this Report

Appthority has analyzed security and risky behaviors from its collection of over 3 million apps and how these apps were being consumed in Enterprise environments. The data measured in this report covers both iOS and Android apps found on BYOD and enterprise devices, as well as additional platforms we have encountered.

Appthority brings together a powerful, automated suite of mobile app risk detection capabilities. By automating the scanning and analysis of employee mobile apps for risky behaviors, hidden actions, and mobile malware, Appthority provides continuous visibility and control over potential security and privacy threats to sensitive company data.

Data points collected include: public vs private apps, Dead Apps that are no longer on the app store, Stale Apps, most popular apps, and new threat campaigns that target the enterprise workplace.

Report Highlights

- Haunted by Dead Apps, consequences of app stores revoking apps
- The latest data from the Enterprise Ecosystem on Apps and OS breakdown.
- Summary of the Mobile Threat Landscape and the latest trends we have come across.
Although Android dominates overall market share of the world’s consumer smartphones, Apple’s iOS overwhelmingly dominates the enterprise market share at 85% of employee devices [based on Appthority proprietary market data]. This can’t only be attributed to employee preference, as not all companies fully embrace BYOD. This may however be attributed to Android’s perceived reputation of being the “unsafe” device.

Google is trying to fight this perception with improved malware analysis capabilities. In it’s 2014 “Android Security Year in Review”, Google states that they’ve reduced Android malware installs by 50%.1 Further, Google has also announced enterprise focused product offerings like Android for Work.2

However, Apple is not sitting still either. Recent partnerships to distribute iPhones, iPads, and apps into enterprise environments, such as their partnership with IBM3 show that Apple does not intend to lose it’s grip on the enterprise any time soon. Further, as we explored in our last app report [www.appthority.com/learn/], iOS apps carry close to the same amount of non-malware risky behavior as Android apps.

Enterprise Mobile OS breakdown

Missing in action?

Missing in action in the enterprise mobility battle are BlackBerry and Microsoft, with only 1% combined market share in the enterprises we surveyed. This is shocking, considering BlackBerry’s past dominance in the space and Microsoft’s ubiquity everywhere else in the enterprise.

Will the introduction of Windows Mobile 10 signal a turn around? While Apple and Google fight for the lion’s share, Microsoft is aggressively trying to crash the party. Microsoft’s largest opportunity is with corporations that do not support BYOD and want to purchase large fleets of devices (corporate assigned devices). Apple is notorious for not offering fleet discounts, Google is fighting a malware perception problem, and Microsoft may come in with heavy discounts to win market share with promised functionality and out of the box connectivity/compatibility to other Microsoft systems in the enterprise.

BlackBerry is also making changes in strategy in order to thrive in the new Enterprise Mobility market. Rather than only support BlackBerry mobile OS, the company’s new MDM (Mobile Device Management) solutions are also able to manage iOS and Android devices.
A look into the Enterprise App Ecosystem

We looked at the apps that were installed most often on enterprise mobile devices and compared them to the top list off iTunes and Google Play. With the exception of a few business apps such as Concur and Cisco Apps for iOS, the usual popular apps (such as Facebook) make their appearances on both iOS and Android. Also absent are games in the list for enterprises, noting they are still there - for example, we did find Candy Crush Soda Saga in the top 50 for enterprise iOS apps (We will be following up with more details on the EMTT Blog including an expanded list of the Top 50 apps in the future)

A major concern related to BYOD stems from the sharing of data. Our findings confirm that these concerns were valid with regard to consumer apps. They can expose corporate information on a device, which increases the exposure risk surface. Phone records, calendars, email addresses and more are accessed and shared with third parties by most consumer apps.

The other concerning observation we are seeing is the lack of any security solutions on most BYOD devices in the TOP 10 list of apps. Only about 4% of Android devices in the Enterprise space had an on-device scanning solution.

Breakdown of the OS/Platforms deployed in the Enterprise Space

- Top 10 Apps most common to the Enterprise
- How this top 10 compares to the consumer-focused app store list

<table>
<thead>
<tr>
<th>Top Enterprise (iOS)</th>
<th>Top App Store (iOS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube</td>
<td>Facebook Messenger</td>
</tr>
<tr>
<td>Facebook</td>
<td>Facebook</td>
</tr>
<tr>
<td>Apple Find My iPhone</td>
<td>Youtube</td>
</tr>
<tr>
<td>Google Search</td>
<td>Instagram</td>
</tr>
<tr>
<td>Concur</td>
<td>Dubsmash</td>
</tr>
<tr>
<td>Cisco AnyConnect</td>
<td>Snapchat</td>
</tr>
<tr>
<td>Pandora Radio</td>
<td>Pandora Radio</td>
</tr>
<tr>
<td>Google Maps</td>
<td>Apple iMovie</td>
</tr>
<tr>
<td>Amazon Kindle</td>
<td>Apple Pages</td>
</tr>
<tr>
<td>Twitter</td>
<td>Apple Numbers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top Enterprise (Android)</th>
<th>Top App Store (Android)</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube</td>
<td>Facebook Messenger</td>
</tr>
<tr>
<td>Google+</td>
<td>Facebook</td>
</tr>
<tr>
<td>Google Maps</td>
<td>Pandora Radio</td>
</tr>
<tr>
<td>Google Play Movies</td>
<td>Instagram</td>
</tr>
<tr>
<td>Gmail</td>
<td>Clean Master (Speed Booster)</td>
</tr>
<tr>
<td>Amazon Kindle</td>
<td>Snapchat</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>Super-Bright LED Flashlight</td>
</tr>
<tr>
<td>Facebook</td>
<td>Go Keyboard</td>
</tr>
<tr>
<td>TripAdvisor</td>
<td>Netflix</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Candy Crush Soda Saga</td>
</tr>
</tbody>
</table>
‘Dead Apps’ are the biggest risk to the Enterprise.

- 5.2% of the iOS apps in an enterprise are dead apps and 37.3% are older versions than the iTunes App Store
- 3.9% of the Android apps are Dead Apps and 31.8% are older versions of what is current on the Google Play App Store

Total Apps in the Enterprise 100

<table>
<thead>
<tr>
<th></th>
<th>Percent of iOS Stale Apps</th>
<th>Percent of iOS Dead Apps</th>
<th>Apps that are current</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>37.3%</td>
<td>5.2%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Percent of Android Stale Apps</th>
<th>Percent of Android Dead Apps</th>
<th>Apps that are current</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>31.8%</td>
<td>3.9%</td>
<td></td>
</tr>
</tbody>
</table>
‘Dead Apps’ are the biggest risk to the Enterprise.

Even though the threat of malware poses a serious concern for mobile devices in the Enterprise, research has identified that there is a more immediate risk to most Enterprise environments. This risk stems from a lack of transparency in the way App Stores handle post release revocation of apps. In other words, when an app is removed from an app store, whether it was for security or vulnerability concerns, violation of app store terms and conditions, developer end-of-life plans, or any other reason, the apps are removed from the app store but remain on users’ mobile devices, in the wild. We have labeled this risk as “Dead Apps”.

A concern with Dead Apps stems from the fact that unlike other consumer product retailers and manufacturers, App Stores at large (Google Play, Apple App Store, Microsoft Windows Store) are under no obligation or regulatory requirements to notify users when they have revoked an app from their store. The reasons for the revocation can vary from copyright infringements to serious security/privacy concerns discovered after release of the app to the store. The notification for the revocation is usually just relayed to the developer of the app who is also not obligated to notify users either. Furthermore, as the app has been revoked from the App Store, the developer is limited in his ability to notify all users of the app and in most cases may just resort to putting a notification on his website if they do anything at all. In a majority of cases, although the apps have been removed from the respective app stores, they can still be found on thousands of user devices.

Despite the fact that Apple and Google have taken significant steps to be more open in the past years, there is still little to no transparency when it comes to the number of apps being revoked from the app stores post release, nor the reasons why the apps were removed. This leaves users who have downloaded the revoked apps in limbo, with lack of any visibility or direction. The fact that the app is no longer available from the respective app stores means they are no longer in a position to be updated for bugs, vulnerabilities, or security fixes. In some cases, the app may have been abandoned or the domains associated with the apps have expired. Dead Apps are also in a position to be exploited by third parties, offering fake updates and content or targeting known vulnerabilities that were never patched.
‘Dead Apps’ are the biggest risk to the Enterprise.

Unfortunately, Dead Apps are not the only concern of its type to enterprise security. There is a similar risk family which we call Stale Apps. Stale Apps are apps that are still available in an app store, but where the version of the app in the app store is newer than the version deployed on user devices. In many cases, users don’t update their apps to the latest versions, even though newer versions may have fixed bugs, patched vulnerabilities, or addressed security concerns. In some cases, users are still running apps that may be several versions old, which represents similar security concerns to the ones brought up by Dead Apps. Fortunately, the fix for Stale Apps is easier to detect, since the app stores notify users of new versions available.

We analyzed hundreds of thousands of apps on enterprise managed devices and found 100% of the surveyed enterprises had both Stale Apps and Dead Apps. For iOS, we found that over a third (37.3%) of total apps were Stale and 5.2% were Dead Apps. Surprisingly we found slightly less on the Android platform with 31.8% of apps Stale and 3.9% Dead Apps.

Google and Apple offer no solutions for protecting the enterprise from these risks. Based on customer demand, Apthority is developing features to allow customers to not only identify Stale and Dead Apps, but also proactively manage remediation actions on employee devices. With the ubiquitous nature of mobile devices the question of should mobile apps be regulated by government arises. Even though the FDA has decided to set the bar when it comes to medical apps, app stores are largely self governed. Should apps be treated like other consumable products? If an app is removed from the market, should app stores be held accountable for transparency? What about the data that was collected by Dead Apps, who ensures that that data is deleted or not put to other use by the author of the app?
Global Look at Mobile Threats

It has been over ten years since the first malware targeting mobile devices was identified in the wild. Since then, there has been close to 4000 mobile families and variants that have been identified targeting mobile devices to date.

Mobile Threat Landscape Summary

- Aprox 4000 Threats/Risks are targeting Mobile Devices
- Biggest risk are from Mobile RAT, Banking Trojans, Spyware

Percentage of Enterprises with Dead Apps: 100%
See EMTR for additional details

Percentage of Enterprises with Stale Apps: 100%
See EMTR for additional details

Emerging Vectors on the Radar
- QR Codes
- NFC
- Battery Drain
- Exploit Kits using Mobile Vulnerabilities
- Affiliate Gangs targeting mobile
- Click Fraud Aggressive Ad Networks
Global Look at Mobile Threats

Evolution

The evolution and functionality of mobile malware can be tied to the evolution of the smartphone and the expanded functionalities of the OS and accompanying hardware. Although the majority of malware families are still profiting from premium SMS scams (a.k.a. Toll Fraud), there is an ongoing shift in tactics resulting in new threat categories such as ransomware and scareware. In addition, hacktivists with remote access tools have expanded the scope of the impacted audience from the consumer space to the enterprise. This evolution is closing the gap between the threat categories that were traditionally considered reserved for the desktop.

Hacktivist pushing the geographical and threat boundaries

Bad actors can be grouped into three categories: “hacktivists,” nation states, and criminals. Hacktivists see themselves as crusaders, using technology to bring about social or political change and/or as a tool for political change, no target is sacred or off limits.

Hacktivists have expanded the boundaries of how technology can be abused, especially on mobile devices. Hacktivists have been responsible for bringing mobile malware to regions such as the US, Iran, Saudi Arabia, Syria, as well regions of China and Tibet. In some of these countries, the traditional economic model of generating revenue from SMS fraud may not formally exist. However, the motivation for hacktivist attacks are seldom financial. The forces at work are driven by targeting specific victims, enterprises, and organizations by what the hacktivists believe to be a higher calling.
Root Exploit use on the decline by malware authors

Although the app sandbox security model can often limit the ability for abuse, it can be bypassed by the use of exploits, like rooting or jailbreaking a device. Three years ago, it seemed that every threat family targeting Android was making use of a root exploit to carry out additional functionality that was otherwise limited by the sandbox model. But, this technique came at a cost; as exploits were based on publicly available code, adding detections around these exploits would render even the most hardened threats immediately detectable. Thus, malware authors would have to make the choice of either sacrificing functionality or stealthiness.

It should therefore not come as a surprise that there has been a significant drop in the number of threat families that employ a root exploit. This highlights the constant evolution of malware techniques, as attackers invest in ways to minimize the detection surface of their apps.

Another driving force is that newer versions of Android are becoming more difficult to exploit, leaving exploits limited to the realm of targeted attacks, where malware development resources can be vast, as is the case with nation states and larger criminal organizations.

Unfortunately, a growing trend is the number of users who are intentionally rooting their devices to gain added functionality that was limited by the OS or device manufacturer. It is really important that enterprises detect and remediate jailbroken and rooted devices, and educate device owners on the risk associated with rooting devices as well as the consequences that could result from such actions.

12 Families in 2012 used root Exploits
0 New families used root exploits in 2015 First Quarter
Global Look at Mobile Threats

Emerging Threat Vectors: Death by a thousand data leaks.

The perception of data breaches in the enterprise has always been associated with the concept of one big breach, where data of a sensitive nature (such as email archives or financial statements) was exfiltrated from a vulnerable server. But, in the context of BYOD, similar results can also be achieved if data is exfiltrated from individual mobile devices that held key information over time. Unlike large data breaches behind the firewall, micro breaches are a lot harder to discover, and it is easier for attackers to cover up their tracks.

An example scenario would be to target a company’s sales force to get a list of their clients. By profiling the sales team using social networks such as LinkedIn and then using social engineering to get them to download seemingly reputable apps, it would be trivial to access their phone contact list/address books.