WHITE PAPER

Improving Mobile Application Store Monitoring and Security

An Osterman Research White Paper

Published January 2014

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

The market for mobile platforms is growing quickly, but the market for mobile applications – most of which are distributed via app stores – is growing at a much faster pace. ABIresearch estimates that 70 billion apps for smartphones and tablets were downloaded during 2013[i].

While most are familiar with the leading mobile app stores – e.g., Apple's App Store, Google Play, BlackBerry World and the Windows Phone Store – there are a large number of third-party app stores, such as Handango, Appitalism, the Opera Mobile Store, Mobile Rated, Getjar and the Amazon Appstore for Android, among many others.

The problem with distributing apps through vendor and third party stores is that there are varying levels of security offered to developers who distribute their apps through these venues. Some app store operations are highly secure and demand that developers meet rigorous standards before their apps can be offered, while others' standards are less stringent. The result is that app stores are susceptible to a variety of security and related problems, such as the distribution of copycat apps and malware distribution. Moreover, some applications are not particularly well written and so are vulnerable to a variety of security problems.

These problems can result in the compromise of companies' brands or intellectual property, the use of apps to distribute malware or other malicious content, theft of customers' login credentials, etc. These problems are particularly acute in the financial services industry, since mobile apps focused on accessing or managing customers' financial accounts carry with them the greatest risk for customers, developers, app store operators and the organizations that distribute these apps.

What organizations need to address these issues is a solution that will scan app stores to look for malware, unauthorized use of brands and trademarks, apps that are connecting to internal systems in an unauthorized fashion, malvertising and other malicious content that could cause damage to an organization.

App stores are susceptible to a variety of security and related problems, such as the distribution of copycat apps and malware distribution.

ABOUT THIS WHITE PAPER

This white paper discusses the results of a survey on mobile app security conducted by Osterman Research. The goal of the survey was to understand the mobile apps that are currently in place, plans for future mobile application offerings, problems with current mobile app store security and the state of current practices focused on security. We surveyed a wide range of industries for the survey, but our focus was on mobile app security in the financial services industry. The white paper also provides a brief overview of RiskIQ™, the sponsor of this white paper.

THE GROWING MARKET FOR MOBILE APPLICATIONS

GROWTH IN THE NUMBER OF MOBILE DEVICES

The mobile device market is expanding rapidly. For example, the Ericsson Mobility Report (June 2013)[ii] forecasts that the number of smartphone subscriptions worldwide will increase from 1.2 billion at YE2012 to 4.5 billion by 2018, representing a compounded annual growth rate (CAGR) of 25%. Growing at a slightly slower pace are mobile PCs, tablets and routers, growing from 300 million in 2012 to 850 million by 2018 for a CAGR of 20%.

INCREASING NUMBER OF APP STORE DOWNLOADS

The market for mobile data and applications – as measured by mobile data traffic – is growing at an even faster pace:

- The Ericsson report anticipates that mobile data growth will increase at a compounded growth rate of 50% per year between 2012 and 2018, from 1.2 exabytes per month in 2012 to 14 exabytes per month by 2018, an increase of 11.7 times in just six years.
- Portio Research estimates that the number of mobile app users worldwide will increase from 1.2 billion to 4.4 billion by 2017[iii].
- Mobile app store use grew from 66 minutes per day in December 2010 to 168 minutes per day in December 2012[iv].
- Pew Research Center found that 50% of mobile phone users download applications, making it the fourth most popular activity for mobile users[v].

By any measure, the growth of mobile devices and apps is increasing at a frenetic pace and shows no sign of letting up.

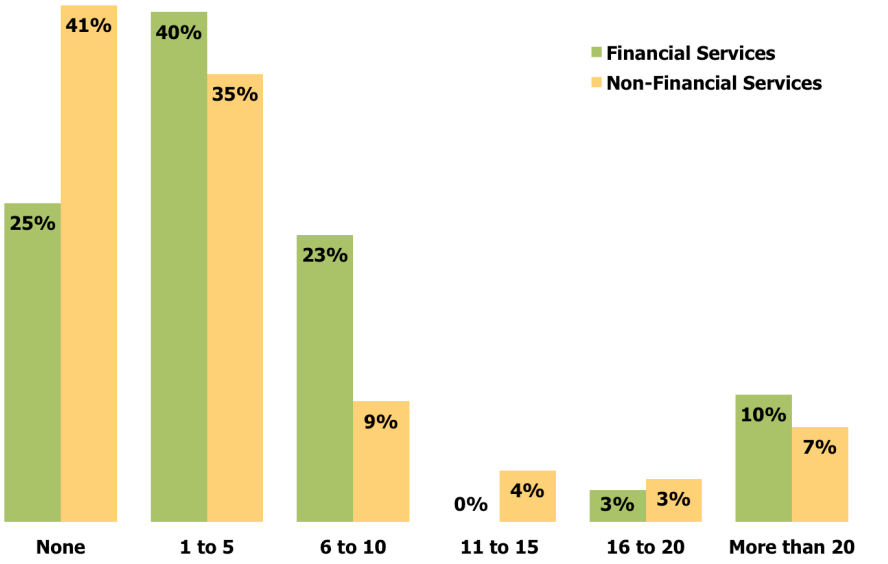
GROWTH IN MOBILE APPLICATIONS

Our research found that many organizations have a small number of mobile apps currently available, but a handful of organizations have more than 20 mobile apps available for distribution, as shown in the following figure. However, our research found that financial services firms have a larger number of mobile apps available for download than do non-financial services firms – 3.1 per financial services firm surveyed compared to 2.5 for firms outside of the financial services industry. We also found that among organizations that have yet to deploy mobile applications, non-financial services firms are twice as likely not to have any plans to deploy them, while financial services firms are 50% more likely to deploy mobile applications in 2014 than their non-financial services counterparts.

In short, our research found that the deployment of mobile apps is, and will continue to be, somewhat more prevalent among financial services firms than among those not serving this industry.

Our research found that financial services firms have a larger number of mobile apps available for download than do non-financial services firms.

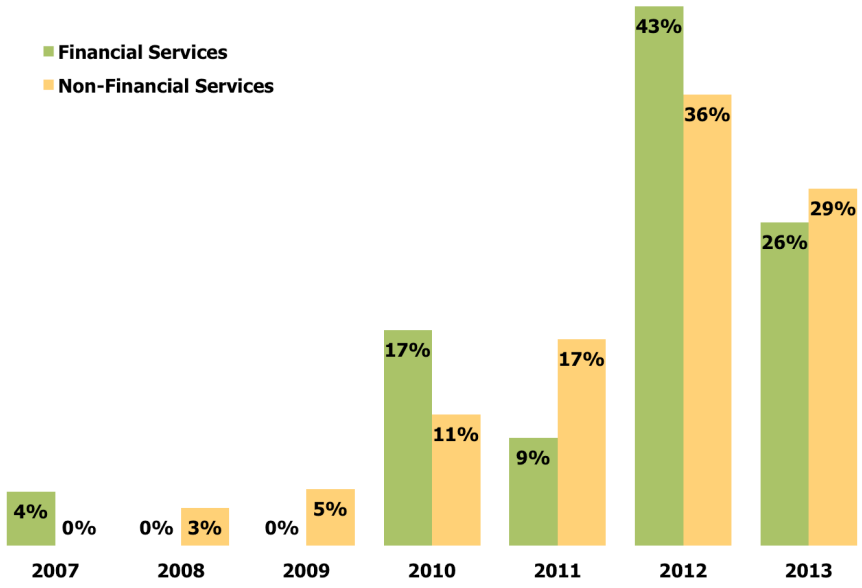
Figure 1
Number of Mobile Applications Currently Available



As shown in the following figure, most mobile apps offered via an app store have been deployed quite recently. For example, most organizations deployed mobile apps

in an app store only in 2012 or 2013, but financial services firms have been even more recent to this market: 79% of financial services began offering mobile apps via an app store in 2012 or 2013 compared to 65% of firms outside of the financial services industry. The result is a relatively short track record in this market, which may explain some of the issues, discussed below, that lead to poor security for mobile apps and app stores.

Figure 2
Year in Which Organizations Began Offering Apps Via an App Store



SERIOUS PROBLEMS WITH MOBILE APPLICATION SECURITY

Malicious mobile apps are a serious problem and one that is growing at a rapid pace. For example, the US Department of Homeland Security and the FBI found that 79% of all mobile malware was focused on Android[vi] (most of the remaining malware is focused on Symbian[vii]). Compounding the growth of the malicious app problem is that most mobile threats are focused on the Android platform. Because Google Play – Google's primary app store – is taking share from Apple's App Store[viii], the problem of malware in the mobile app space is likely to get much worse.

Malicious mobile apps are a serious problem and one that is growing at a rapid pace.

One of the problems with Android from a malware perspective is its fragmentation – i.e., the large number of Android versions currently in use, some of which are less secure than others. For example, for the seven-day period ending December 2, 2013, the distribution of Android operating systems in use were[ix]:

- Jelly Bean (4.1.x): 37.4%
- Gingerbread (2.3.3-2.3.7): 24.1%
- Ice Cream Sandwich (4.0.3-4.0.4): 18.6%
- Jelly Bean (4.2.x): 12.9%
- Jelly Bean (4.3): 4.2%
- Others: 2.8%

The fragmentation in the Android space, which is significantly greater than for iOS, contributes to the mobile malware problem because cybercriminals can impact a large proportion of Android users who are using older and less secure versions of the

operating system. For example, as of early December 2013, only 1.1% of Android users employed KitKat (v4.4), the most recent version of Android.

The seriousness of malicious mobile apps distributed via app stores impacts both users who are the targets of cybercriminals and who stand to lose significant amounts of money from malware that might, for example, access their banking login credentials. Malicious mobile apps also impact app providers in whom customers might lose trust if malicious apps are able to compromise customers' sensitive or confidential information.

THREATS ARE NUMEROUS AND VARIED

There are a number of threats that can impact mobile apps:

- **Copycat applications**
  Copycat apps are what their name implies – apps that are designed to look and feel like legitimate apps, but that are designed for a variety of malicious purposes. For example, a malicious developer can easily disassemble an existing app and repackage it so that it looks similar or identical to a legitimate one, but they will include code that will add spam or other advertising in the app interface, implement a capability to steal login credentials, or send for-fee SMS messages that will add charges to their wireless bill. RiskIQ's analysis of more than five million mobile apps has revealed that in excess of 90% of leading brands have had their apps copycatted.

  The impact of copycat apps on users and legitimate developers can be significant. Users can have their login credentials for financial accounts stolen and, potentially, their accounts drained as a result of doing nothing more than logging in to view their financial records or transfer funds. Legitimate developers also lose because users will mistakenly download an app thinking it to be genuine, and thereby prevent a sale for the developer whose app they actually wanted to download. For example, at one time there were four copycats of the game Riptide GP 2 available on the Google Play store, which the original developer estimates cost the company anywhere from $6,000 to $31,000[x] in lost sales.

- **Stolen applications**
  Closely related to the problem of copycat apps are stolen applications that are available from illegal app stores. One source estimates that the Chinese iOS app market, for example, generates more than $10 million annually from stolen apps, many of which are used on jailbroken phones[xi]. Because these apps are available from unauthorized app stores, they are more susceptible to malware infection because they bypass the controls that Apple's official app store imposes.

- **Data leakage**
  Another quite serious problem with many mobile apps is the propensity for many of them to leak sensitive or confidential data. While this is more common with free apps, it is also a common problem with paid ones, as well. One mobile security vendor discovered that 95% of the leading 100 free mobile apps are prone to data leakage, but paid apps are not far behind in terms of the risk they pose to the privacy of customer information[xii]. It is important to note that data leakage is not typically the result of bugs in software – rather, it is the result of app developers capturing potentially sensitive information, such as users' geographical location or their identity, and not preventing the distribution of this information.

- **Malware**
  Mobile app-focused malware is becoming increasingly common, most of it (but not all) directed against Android devices. Mobile malware can carry out a variety of malicious tasks, such as sending premium SMS messages that charge the user and then prevent the display of a receipt or confirmation on the mobile device, modify users' search results so that they are directed to advertisers who pay

Mobile app-focused malware is becoming increasingly common, most of it (but not all) directed against Android devices.

malware developers as part of mobile adware campaigns, or steal information about users.

- **Excessive number of application permissions**
  Some mobile apps require a significant number of permissions before they can be installed. For example, a beta version of the Facebook App for Android v4.0.x requires several different permissions, including the ability to connect or disconnect from Wi-Fi networks, access to users calendars for the purpose of adding or modifying events, and the ability to read users' text messages[xiii]. Requiring an excessively large number of permissions can not only compromise users personal information, but it can create more egress points for sensitive or confidential information, such as when users log into their financial accounts.

- **Authentication**
  Another serious issue with mobile app security is user authentication. Mobile devices, by the nature of their small size compared to laptop or desktop computers, present more difficulty to users when entering passwords. Consequently, many applications employ Personal Identification Numbers (PINs) instead of usernames and passwords. However, while PINs are easier to enter than text, they are relatively easy to guess because about one-quarter of PINs are a spouse's birthday date[xiv]. Still, PINs are preferable to passwords, largely because mobile devices use auto correction when entering text, making their entry tedious and time-consuming (about 20-30 seconds for the typical password on a mobile device). Adding to the problem is that good, secure passwords are difficult to remember simply because they are odd – the more secure the password, the more difficult it is to remember.

The bottom line is that all of these problems create an increase in overall corporate risk in three important ways:

- Network security can be compromised. For example, malware on a mobile device can infect corporate systems when a user logs into them via their mobile device. Osterman Research has found that 36% of mobile users employ their primary mobile device to share content with partners, customers and prospects; and that 97% use this device to check email.

- Similarly, sensitive or confidential data assets can be compromised when users login to business systems using compromised mobile devices. This can create enormous problems for an organization if protected health information (PHI), personal financial information (PFI) or intellectual property is stolen.

- Aside from the problems that individual users or organizations can experience from the variety of problems discussed above, compromise of PHI, PFI or other sensitive information can result in various regulatory and/or legal problems. For example, inadvertent loss of PHI because of poor mobile security can result in violation of the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA), or violation of US regulation 45 CFR 164.530(C)(c)(1), which states that "a covered entity (e.g., a hospital or clinic) must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." Loss of PFI can violate the requirements of the Payment Card Industry's Data Security Standard (PCI DSS) or the Gramm-Leach-Bliley Act. Data loss can also result in significant penalties and sanctions as part of legal actions that may be brought against compromised organizations.

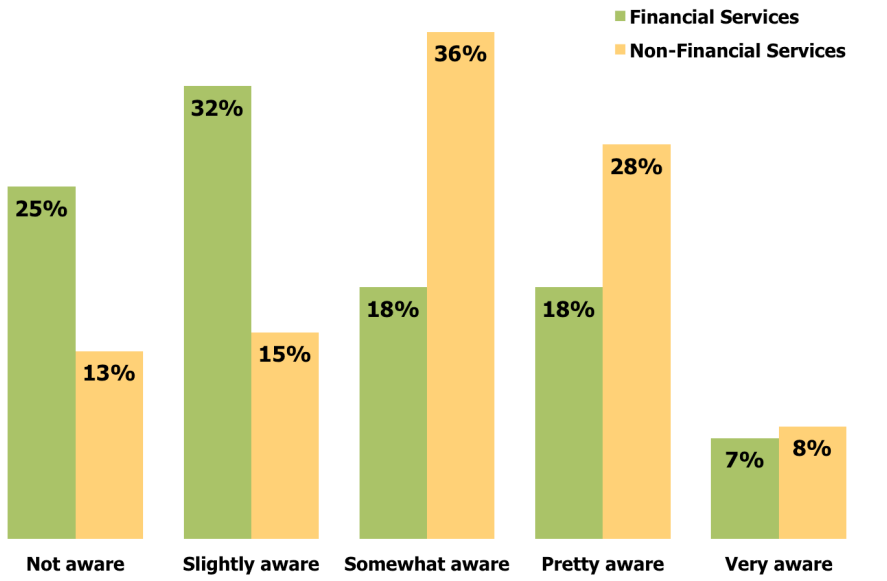
Inadvertent loss of PHI because of poor mobile security can result in violation of the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA).

SECURITY PRACTICES ARE LACKING

LACK OF AWARENESS

Our research found some serious problems among organizations that distribute their mobile apps via app stores. For example, as shown in the following figure, a significant percentage of app managers are either completely or largely unaware of security issues that may exist on mobile app stores, while a smaller proportion are quite aware of these problems.

Figure 3
App Manager Awareness of Security Issues on Mobile App Stores



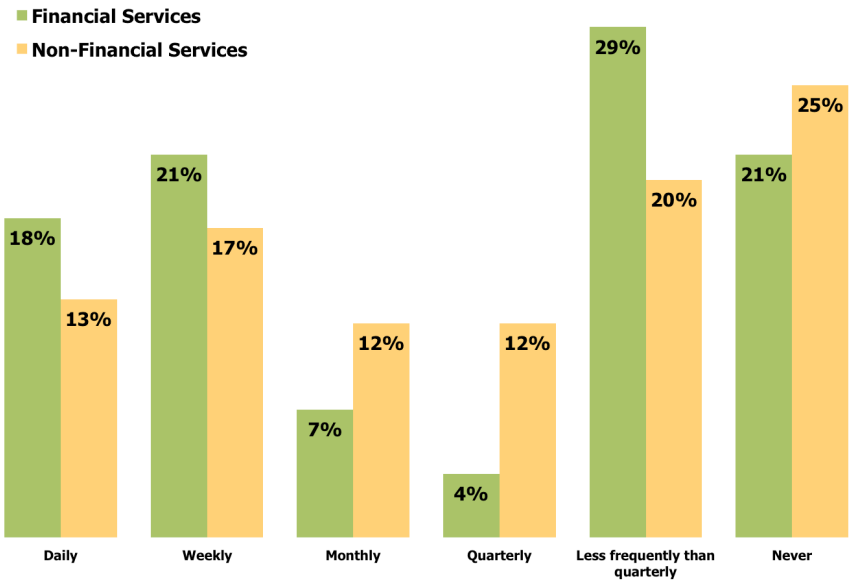
Arguably, this is the most significant problem we found in our research: managers and other decision makers that are not aware of the various security-related issues in the app stores through which they distribute their mobile apps are unlikely to implement the technologies and practices necessary to protect their customers from the variety of serious problems that can result from poor security.

APPLICATION STORE SCANS DO NOT OCCUR WITH SUFFICIENT FREQUENCY

Another serious problem we discovered is that the organizations' frequency of scanning mobile app stores to check for rogue or malicious apps that might target their customers is sorely lacking. For example, as shown in the figure below, 21% of financial services firms that distribute mobile apps and a slightly higher proportion of non-financial services firms never scan for problem apps. At the other end of the spectrum, fewer than one in five financial services firms and only one in eight firms outside of this industry scan for problems on a daily basis.

Fewer than one in five financial services firms and only one in eight firms outside of this industry scan [mobile apps] for problems on a daily basis.

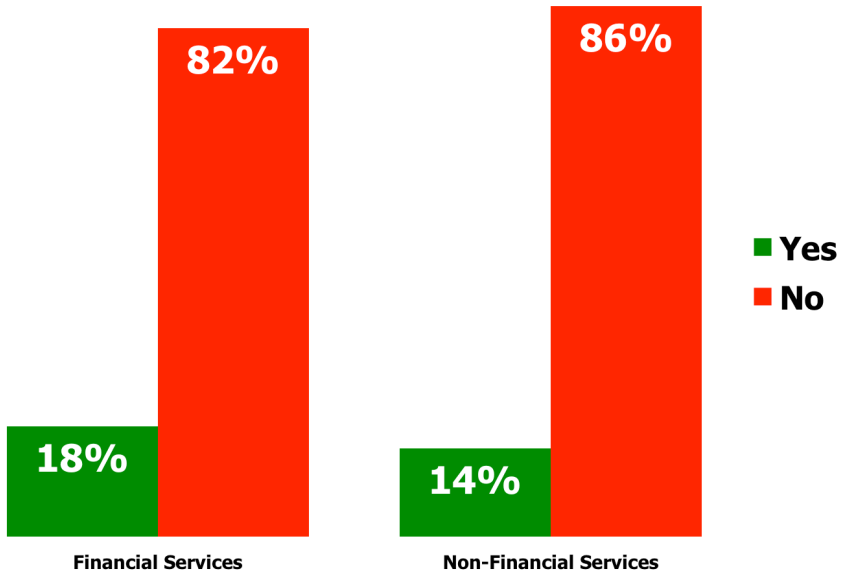
Figure 4
Frequency of Scanning Mobile Application Stores to Check for Rogue or Malicious Apps Targeting Organizations' Customer Base



One of the key reasons for the infrequent nature of mobile app store scanning is that relatively few organizations have deployed a solution that will monitor application storage for the inappropriate, unauthorized or illegal use of organizations' brands or for the malicious intent for which a mobile app may have been designed, as shown in the following figure.

Relatively few organizations have deployed a solution that will monitor application storage.

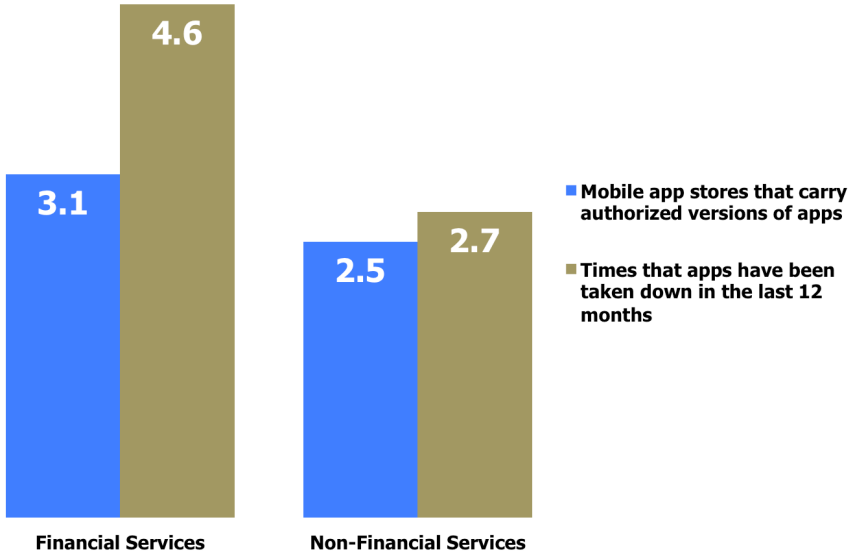
Figure 5
"Has your organization deployed a solution that monitors application storage for usage of your brand and malicious intent?"



THE RESULT: POOR APP STORE SECURITY

The combination of a lack of awareness of mobile app and app store security issues, coupled with relatively infrequent scanning for rogue or malicious apps results in the need to take down apps on a somewhat frequent basis. For example, as shown in the following figure, financial services firms have more mobile apps in distribution than their non-financial services counterparts, but experience a much higher degree of app takedowns. Our research found that during the previous 12 months, 20% of financial services organizations have had to take down and/or enforce a corporate policy against a malicious mobile application that had targeted their customers.

Figure 6
Relationship Between Number of Mobile App Stores that Carry Authorized Versions of Apps and Times That Apps Have Been Taken Down in the Last 12 Months

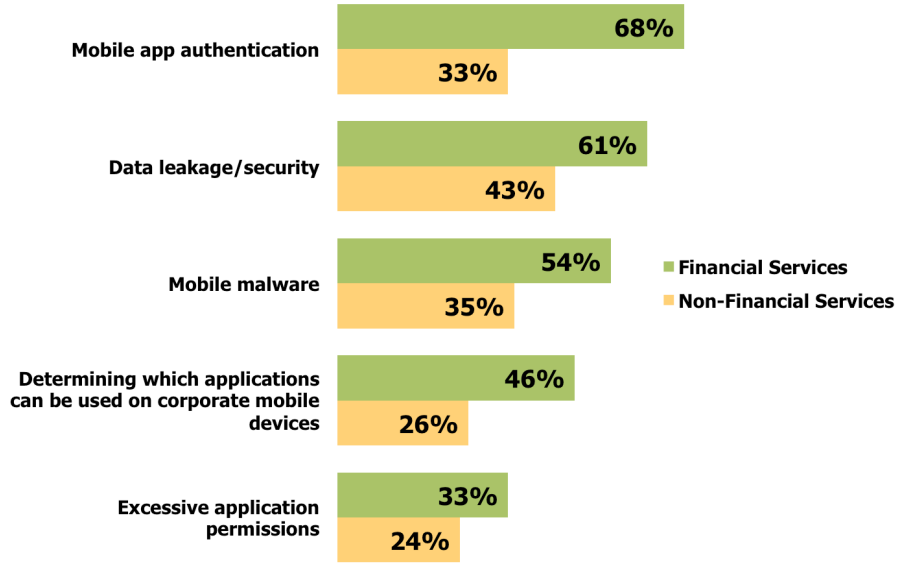


THE GOOD NEWS

Despite the lack of awareness about the depth of the mobile app store security problem by some decision makers, the lack of app store scanning that takes place and the frequency with which apps must be removed from app stores because of security problems, most decision makers – particularly in the financial services industry – really do understand the need to improve the status quo. For example, as shown in the following figure, two-thirds of organizations in the financial services industry consider mobile app authentication to be a serious or very serious issue. Similarly, three out of five view data leakage/security issues to be this serious, and most view mobile malware as a high priority issue that they must address.

Financial services firms have more mobile apps in distribution than their non-financial services counterparts, but experience a much higher degree of app takedowns.

Figure 7
Severity of Various Mobile App Store Security Issues
% Responding Serious or Very Serious



RECOMMENDATIONS

Osterman Research offers three recommendations for organizations that distribute mobile apps via app stores:

- **Understand the problem**
  First and foremost, decision makers in organizations that distribute mobile apps via app stores need to understand the depth of the problem they face. This is nowhere more important than in the financial services industry, since cybercriminals heavily target this industry because of the significant potential for stealing funds from unsuspecting customers' financial accounts. While understanding the depth of the problem may seem obvious, our research found that many decision makers are not aware of the severity of the problems that they may encounter when serving the mobile app store marketplace.

- **Implement appropriate safeguards**
  Next, any organization involved in the mobile app marketplace must implement appropriate safeguards to ensure that their applications are as safe as possible for their customers to use. This includes creating a set of application development guidelines that will help internal or contract developers to build applications that are as safe as possible. Organizations should also conduct regular security reviews to ensure that apps are being developed according to these guidelines, and that they are designed to address new threats as they arise.

- **Deploy a robust security solution**
  Finally, every organization that distributes mobile apps via app stores should implement a robust mobile app security solution that will enable them to protect their brands, trademarks and other intellectual property; that will address copycat applications that attempt to fool customers into downloading impostor applications; that will address malvertising issues in order to protect customers from spam and other malicious content; and that will address malware and other threats.

Any organization involved in the mobile app marketplace must implement appropriate safeguards to ensure that their applications are as safe as possible for their customers to use.

SUMMARY

Mobile apps distributed via app stores can provide significant benefits and competitive advantage to organizations that offer them. However, these apps – particularly those focused on the financial services industry – also attract cybercriminals and others with malicious intent. Malicious activities can damage an organization's brand, allow customers' data security and privacy to be compromised, and can negate much of the benefit that organizations hope to achieve by distributing mobile apps via app stores. Consequently, all organizations that offer mobile apps via app stores should have the processes and technology in place to address malicious activity and prevent, to the extent possible, the compromise of their brands and intellectual property, as well as their customers' data and finances.

ABOUT RISKIQ™

RiskIQ™ is a leading provider of enterprise security solutions beyond the firewall. The company's proprietary Virtual User technology intelligently interacts with websites and mobile applications, modeling end user behavior to trigger and detect anomalies, policy violations and previously undetected threats. A global proxy network scans millions of web pages and mobile applications daily, providing some of the world's largest financial and technology companies unprecedented visibility and control of critical assets distributed beyond their corporate borders

RiskIQ™ provides the following solutions to help companies address the problem of visibility and control of their web and mobile assets.

MOBILE APPLICATION SECURITY

As the number of mobile apps and the stores that distribute them come and go, it becomes a resource intensive challenge to maintain control of your apps across all these touch points. RiskIQ automates the discovery of your mobile apps and partner apps and helps you focus on your critical assets. By leveraging our MobileDB of 5+ million mobile apps, we help companies identify immediate threats and automatically take down unauthorized apps using their brand or connecting to their IT systems.

WEBSITE SECURITY

With more than 4.5 billion pages across 650 million unique websites in existence today, it is a challenge to keep a pulse on one's web footprint and ensure the security of all associated web assets. With a unique approach to scanning the open web, RiskIQ can quickly determine an organization's ownership of web assets and their respective dependencies. Once these assets are discovered, they can be brought under management for continuous monitoring. Because of our expansive coverage of the web, we detect emerging threats before they can do major damage to a company's online brand.

MALVERTISEMENT AND MALWARE PREVENTION

Because there are so many players in the ad supply chain, websites that run third-party ads don't have much control over what ads are displayed to their visitors. RiskIQ intelligently scans and tracks advertisements as they traverse through the ad supply chain. We detect, classify and report on suspicious activity and confirmed malvertisements, notifying advertising operations team in real-time with detailed forensics of events uncovered.

BRAND AND TRADEMARK PROTECTION

RiskIQ monitors the web for trademark misuse and abuse, prioritizing these incidents based on their monetary impact to a business and brand. Our comprehensive solution spans both emerging and targeted content -- the advertisements, blogs, mobile apps, and websites that have the greatest chance of reaching and influencing a company;s current and potential customers.

All organizations that offer mobile apps via app stores should have the processes and technology in place to address malicious activity.

REFERENCES

[i] https://www.abiresearch.com/press/android-will-account-for-58-of-smartphone-app-down
[ii] http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-june-2013.pdf
[iii] http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e
[iv] http://www.andmine.com/blog/mobile-app-statistics-2013-usage/
[v] http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx
[vi] http://blog.malwarebytes.org/mobile-2/2013/09/79-percent-of-malware-is-directed-at-android/
[vii] http://www.mercurynews.com/troy-wolverton/ci_24438125/wolverton-if-youre-running-android-watch-out-malware
[viii] http://www.pcmag.com/article2/0,2817,2428691,00.asp
[ix] http://developer.android.com/about/dashboards/index.html
[x] http://securitywatch.pcmag.com/mobile-security/316843-mobile-threat-monday-leaky-document-signing-apps-and-ad-packed-plagiarized-apps
[xi] https://medium.com/design-startups/374a4f06c903
[xii] http://www.eweek.com/mobile/top-mobile-apps-overwhelmingly-leak-private-data-study/
[xiii] http://theonlycog.com/facebook-excessive-permissions
[xiv] Source: Dr. Marcus Jakobbsson, principal scientist at PayPal