IBM Software
Thought Leadership White Paper

January 2014

What can you do differently to guard against threats from rapidly evolving mobile malware?

Extending security protection from traditional, web-based applications to mobile applications

IBM

Introduction

Just when you thought it was safe to go mobile, everything is different.

The risks are different. Only a few years ago, predictions stated that smartphones and tablets had little vulnerability to malware and hacking. But in the one-year period ending March 2013, malware aimed at mobile platforms grew 614 percent, nearly 450 percent faster than a year earlier.[1]

The pervasive nature of risk is different. Of the top 100 paid mobile applications, 100 percent on the Google Android platform and 56 percent on Apple iOS have been hacked. Among popular free applications, 73 percent on Android and 53 percent on iOS have been hacked.[2]

But in today's business climate, you cannot avoid going mobile. Companies, employees and customers expect the convenience and productivity of anywhere, anytime connectivity and data access. In fact, signs indicate that despite growing security risk, organizations are becoming increasingly mobile, not less mobile.

So in today's different world—the mobile world—what do you need to do differently?

This white paper will discuss the risks that accompany mobile computing and applications, explain what's different between threats to mobile and conventional devices, point out users' behaviors that pose risk, and present solutions to help address the risks and vulnerabilities that make mobile applications susceptible to mobile malware.

What's different about today's threats and attacks?

Put yourself in a hacker's shoes. You're looking for financial gain—and stealing data is one way to accomplish that goal. Conventional IT infrastructures have long been the battleground. But you see growing opportunity in the rapidly evolving use of mobile devices. Already, 69 percent of employees access business networks using personal mobile devices.[3] By 2015, some 40 percent of all devices used in enterprise environments are projected to be mobile devices.[4]

Mobile devices—especially smartphones or tablets utilized in bring-your-own-device (BYOD) environments—provide particularly attractive targets. They typically contain personal and business data that hackers can mine and sell. But applications on mobile devices also provide access to enterprise networks that can be even more lucrative. While security threats to mobile devices typically involve relatively small amounts of private data along with activities such as phishing or unauthorized phone calls, the overall threat to the enterprise can be significant data leakage.

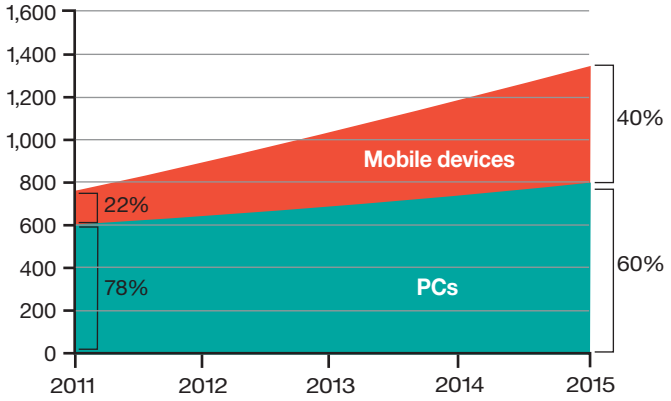
What's different about how attacks work?

Here's how it works. Attackers download mobile applications from app stores and reverse engineer them to identify security vulnerabilities. Then they create malware to take advantage of those vulnerabilities and infect applications on mobile devices. They distribute the malware via websites, email or other means so it can infect applications after installation—or they place malware-infected applications in app stores that users visit for downloads. One study has identified more than 500 third-party Android app stores worldwide that host mobile applications infected with malware.[5]

Once on users' devices, the malware can perform a number of functions, from intercepting authentication credentials to disabling encryption. It can even gather information stored on the device and send it to an attacker.

But today's sophisticated malware carries a particular danger. Working from an infected application, it can search for vulnerabilities in other applications on the device—usually proprietary enterprise applications that the attacker has not previously been able to access. When it locates such a vulnerability, the malware can exploit it for unprecedented access to valuable and sensitive data.

Growth in enterprise devices by type



Source: IBM projection

What's different about how enterprises respond?

In 2011, smartphone sales exceeded PC sales for the first time.[6] And as the number of mobile devices has grown and their use has evolved, so have approaches to mobile security—from virtually no awareness or attention in the 1990s, to reactive responses in the 2000s meant to address attacks that had already occurred, to today's proactive approaches for preventing future attacks.

In fact, a recent global study of more than 4,600 IT and IT security professionals found that 74 percent of respondents say employee use of mobile devices poses a serious risk. But many organizations have done little about it. According to the survey, 65 percent of organizations have no policies regulating employees' use of mobile devices, only half require security settings on mobile devices, and only three percent of those requiring security say that all of their employees are compliant.[7]

Consequently, in the year leading up to the survey, 60 percent of respondents experienced an increase in malware infections and 51 percent had experienced data breaches—all due to the use of insecure mobile devices.[7]

What are the different perceptions of danger?

A recent tally by the Open Web Application Security Project (OWASP) of the top 10 mobile risks placed "insecure data storage" at number one.[8] But "insecure data storage" can be a danger for two very different reasons—when a device is lost or stolen, and when malware attacks. A focus on the wrong reason can sidetrack the organization from providing the kind of protection that's necessary in today's mobile environments.

In fact, that is often the case. Among respondents to a recent survey, 78 percent said lost or stolen devices were their top security concern. Meanwhile, the fear of users downloading malware-infected applications was the number three concern, at only 34 percent. The danger of malware attacking proprietary applications developed in-house stood at only 19 percent, as concern number eight.[9]

Of these dangers, however, the one that is least feared—attacks to proprietary applications—is actually the most significant. The need for security in internally-facing applications is poorly understood, yet an attack on applications can yield access to hundreds or thousands of mobile devices and their application-based data. This lack of understanding can create a security gap that hackers can easily exploit.

Why do these different perceptions pose a risk?

Not only is mobile computing on the rise, so is the trend to permit employees to use their own smartphones and tablets at work. Some 68 percent of organizations have enacted BYOD policies, an increase from 62 percent in 2012.[8] One study projects 38 percent of organizations will stop supplying company-owned devices to employees by 2016—and that by 2017, half of all organizations will require employees to provide their own devices.[10]

The upshot is that, aside from losing information that resides on the device, what happens in a loss or an attack to the physical device is regarded as a greater concern for the employee than for the organization. It's the employee who has to purchase a new smartphone or tablet.

But the organization should still worry about a greater, and often underestimated, concern—the applications residing on the device. That's because it is more efficient for attackers to use mobile malware to mine and capture data than to depend on the occasional loss or theft of a smartphone. Malware that surfaces either via an infected download or through web-based or email phishing attacks can capture sensitive information that can give them access to the huge volumes of data on servers and across all devices where the applications are installed.

What makes mobile threats different from threats to PCs?

Attacking and stealing enterprise data via applications can happen on any device—mobile, desktop or even a server. But mobile computing has a number of characteristics that make it particularly vulnerable to exploitation—and attractive to purveyors of malware.

Importantly, mobile users engage in behaviors that make it easy for malware to find its way onto the device. Mobile devices are used in more locations, often with connections that are not secure. Devices and applications are diverse, making them difficult to manage. Devices are often shared, requiring complex authentication.

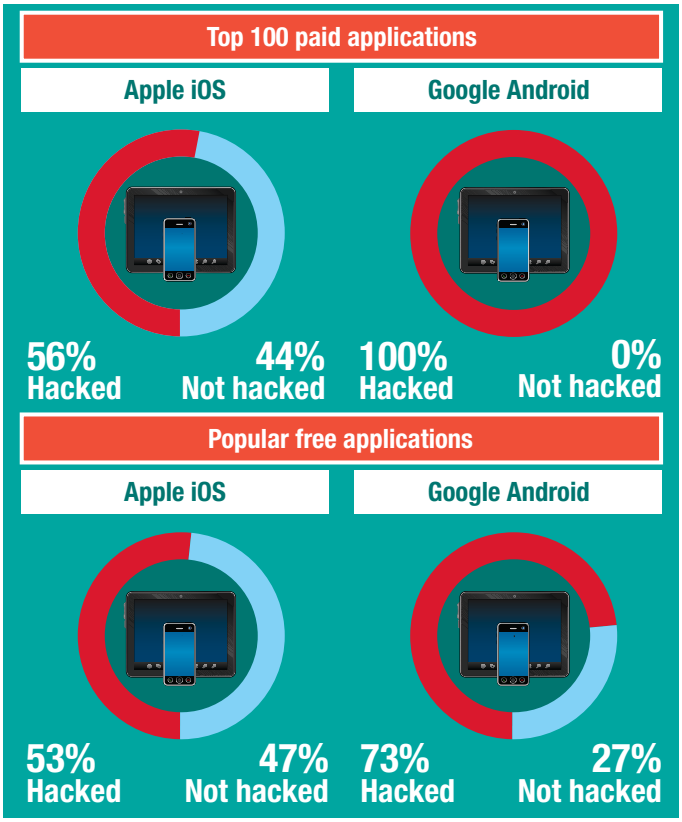
What is more, with mobile smartphones and tablets rapidly becoming the everyday device of choice, many people casually download large numbers of applications from various sources and pay scant attention to security concerns.

With device use typically more personal, rapid and trusting than in PC-dominant environments, users frequently don't notice which version of an application—perhaps an infected version—they are downloading.

Mobile users often do not understand the permissions they are granting when they install an application or visit sites that are accessible via a quick response (QR) code. They frequently click through security warnings to get to the content they want quickly—automatically clicking "Yes," for example, to accept Facebook applications that essentially control their phones and even post to Facebook on their behalf.

Yet universally allowing permissions or going to sites unseen can open the doors wide to malware. This malware can then introduce security risks to enterprise applications and data that also reside on the device.

No one is spared: Malware attacks all mobile platforms



Source: "State of Security in the App Economy: Mobile Apps Under Attack," Arxan, 2013.

What's different about the defenses you need?

In response, organizations need to recognize these behaviors and follow industry best practices designed to control them and to mitigate risk. Organizations need to establish education programs to ensure that users fully understand the dangers of malware—and the actions that can lead to malware infection.

At the same time, they need to continue practices such as the use of firewalls and intrusion prevention systems that help secure mobile and conventional infrastructures.

However, out of fear of upsetting users who want to control the devices they own, organizations typically place few controls on the applications that users themselves install, despite the fact that virtually any application—free or purchased, business software or games—can be infected with malware.

So to combat malware that does find its way onto the device and then onto business applications on the device, the organization needs technologies and practices that address underlying vulnerabilities of applications and enhance data and application security.

What should you do differently for the protection you need?

Mobile security is about protecting more than the device. It is about protecting applications and data on the device. It is about detecting data leakage, recognizing what information is being sent to unauthorized locations, identifying those locations, and precluding malware attacks before they can steal valuable information.

IBM® Security AppScan® provides an application security solution that can determine application vulnerabilities early in the software development lifecycle—identifying vulnerabilities and generating intelligent fix recommendations so business applications arrive on the mobile device less vulnerable to exploitation by malware.

Supporting both Google Android and Apple iOS native applications, AppScan identifies where data enters an application, where it goes inside an application and where it leaves an application. This comprehensive analysis helps to quickly identify data leakage and to ensure sensitive information is protected.

Addressing both the mobile and server components of applications, and using the same techniques to scan applications in development for mobile devices that are used to scan applications for traditional computers, AppScan helps organizations secure the complete application environment to preserve not only the flexibility and empowerment mobile users expect but also the security the enterprise requires.

For more information

To learn more about IBM Security AppScan, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/appscan

[5] "Juniper Networks Finds Mobile Threats Continue Rampant Growth As Attackers Become More Entrepreneurial," *Juniper Networks*, June 26, 2013. http://newsroom.juniper.net/press-releases/juniper-networks-finds-mobile-threats-continue-ram-nyse-jnpr-1029552

[6] Alex Cocotas, "Smartphone Market Forecast: Sales Will Exceed 1.5 Billion Units a Year by 2016," *BI Intelligence*, February 2012. http://www.businessinsider.com.au/smartphone-market-forecast-sales-will-exceed-15-billion-units-a-year-by-2016-2012-2

[7] "Global Study on Mobility Risks. Survey Results for: United States," *Ponemon Institute*, February 2013. http://www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf

[8] "OWASP Mobile Security Risks: Top 10 Mobile Risks," *Open Web Application Security Project*, 2012. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

[9] Michael Finneran, "2012 State of Mobile Security," *InformationWeek*, May 2012. http://www.ihrim.org/Pubonline/Wire/June12/2012-state-of-mobile-security.pdf

[10] "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes," *Gartner, Inc.*, May 1, 2013. http://www.gartner.com/newsroom/id/2466615

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2014

[1] Juniper Networks Mobile Threat Center, "Third Annual Mobile Threats Report: March 2012 through March 2013," *Juniper Networks*, 2013. http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf

[2] "State of Security in the App Economy: Mobile Apps Under Attack," *Arxan*, 2013. https://www.arxan.com/assets/1/7/State_of_Security_in_the_App_Economy_Report_Vol._2.pdf

[3] IBM projection.

[4] Michael Finneran, "Research: 2012 State of Mobile Security: Mobile Security a Work in Progress" *InformationWeek*, May 2012. http://reports.informationweek.com/abstract/18/8792/Mobility-Wireless

WGW03053-USEN-00