Securing The Enterprise From Mobile Malware
Foreword

In the cyber security space, malicious software, or “malware,” is a top concern, as it cripples businesses, damages networks and stymies the enterprise professional. It is an umbrella term that includes viruses, ransomware, adware, etc. When left unrestrained, it acts against computer users’ requirements and performs illicit functions like copying, spying and retrieving.

Although antivirus software and firewalls have been deployed for most companies, cyber-criminals have become relentless, stopping at nothing less than complete infiltration.

So, what solutions and practices can be utilized to combat malware? This report will touch upon methods such as multi-factor authentication (MFA) and access controls, patches, application awareness, software as a service (SaaS) options and more.

More specifically, this report will evaluate facets of today’s threat landscape. As pernicious malware propagates on networks worldwide, security experts are examining mobile connectivity. While malware campaigns are somewhat less frequent on the mobile front, they are quite dangerous, nonetheless.

As mentioned, then, this report will trace hacker motives, and vectors, discuss particularly harmful attack methods, and shed light on the road ahead. Security experts will prognosticate, giving their take on the threat landscape, exploited apps, best practices and more.

Have you ever wondered how “bring your own device” (BYOD) endpoints impact the enterprise? Read on to find out. What’s more, have you questioned the lengths threat actors will go to hijack devices and wreak havoc on various users? We review these antics, and stack mobile infiltration beside desktop and laptop offensives – in an effort to illuminate all corners of today’s attack surface.

Table of Contents:

3 Background On Mobile Malware
4 Mobility As A Security Concern
5 Mobile Weak Spots
6 Shoring Up Mobile Defense
7 Microcosm Of The Threat Landscape
8 Sponsor Spotlight
9 About Cyber Security Hub
Background on Mobile Malware

It should come as no surprise that phishing remains the steepest climb for security professionals when it comes to mobile devices. The method remains a top choice for today’s threat actors looking to exploit a laptop or endpoint. PhishMe’s 2016 Enterprise Phishing and Susceptibility and Resiliency Report showed that 91% of cyber-attacks and the “resulting data breach begin with a spear phishing email.”[1] Today’s CISO, then, must monitor the network’s endpoints, but also be fluent in business language – to relay the burgeoning mobile threat to upper management.

Mobile connectivity has proven earth-shattering for the consumers that operate smartphones, but for those using BYOD or corporate devices, they may be a direct route to an enterprise’s “crown jewels.” Tiered systems formerly set up in the enterprise to repel hackers have proven ineffective. Nefarious actors have breached strengthened firewalls. The will of the hacker grows alongside network defense efforts. So, the quantity of data breaches continues to rise.

In many cases, hijacked mobile devices, with a subsequent malware payload, are the catalysts of that rise. According to a Check Point Software survey, 20% of companies polled said their mobile devices had been breached and 94% expected the frequency of mobile attacks to increase. [2]

What’s more, according to Telecom Asia and Pradeo Labs, there has been a 92% rise of zero-day malware on mobile devices in the past six months. [3] It seems, then, that hacker focus has indeed shifted to enterprise mobility, at least in part. It also indicates that hackers are constantly improvising, so Chief Information Security Officers (CISO) and the like must stand guard around all facets of the network – from PCs to endpoints, to their point solutions and more.

While the number of assaults through the network remain constant, there has been a 100% growth in instances of device compromise in the last six months, illustrating that the threat landscape is constantly shifting.

Zero-day malware references strains previously unknown to databases and detectable only via real-time analysis. Pradeo Labs’ Mobile Threat Report highlights three prominent vectors with regard to the mobile issue: applications (malware, spyware, adware), the network (phishing, Man-In-The-Middle (MATM) attack) and the device (OS vulnerabilities).

The study revealed a common denominator and that’s the threat of data exfiltration via mobile applications. Mobile malware is far less frequent, but it can damage more terrain in its path. The report read: “While the number of assaults through the network remain constant, there has been a 100% growth in instances of device compromise in the last six months, illustrating that the threat landscape is constantly shifting.”

The study points to data leakage via applications (credentials, profiles and SMS messages) as a crux of enterprise activity. Further, it stated: “As governments and authorities urge organizations around the world to protect personal data from leakage and theft, mobile applications are a big risk for compliance and their behaviors must be scrutinized.”

Mobility As A Security Concern

The Indian English-language newspaper Deccan Chronicle recently published a report debunking mobile security myths.\[4\]

In prefacing their overarching points, the outlet wrote: “As an unwitting employee uses their compromised device and logs into corporate systems containing sensitive data, cyber criminals may collect their usernames and passwords. Then, they can exploit unsecured networks, infecting other mobile devices, stealing, or changing data. They can even install malicious apps that give them virtually unrestricted access to a device and its data.”

The first, and perhaps most striking, myth: “Mobile isn’t a big problem.” On the soaring number of overall cyber incidents pegged to mobile, Deccan outlined malware efforts and malicious Wi-Fi networks.

Further, it captured the strong need to protect endpoints within the banking, financial services and insurance (BFSI) space, writing: “Banks understand the threat and are more likely to invest in mobile security. When asked to identify their top five challenges, 60% (of respondents to a recent survey) of bank CIOs said, ‘Keeping up with security issues.’”

Similarly, a recent survey of the Cyber Security Hub audience underscored the rising awareness – and prominence – of enterprise mobility. Asked which industry topics they follow the closest, 44% of nearly 200 respondents (active security practitioners) indicated “mobile security.” There’s no doubt that mobility remains top of mind.

Piggybacking off this, and following coverage of iOS “immunity” and mobile device management (MDM) and enterprise mobility management (EMM) solutions, Deccan also wrote: “(Mobile devices) cannot use the same advanced detection techniques (as antivirus products for PCs and laptops) due to a mobile device’s limited performance and battery life. Mobile antivirus solutions are limited compared to their PC cousins. They can uncover malicious code in apps by looking for unique binary signatures that identify known malware.”

However, the report indicates that “criminals have found new ways to obfuscate those signatures, making them useless in the detection of mobile malware... At best, antivirus protection detects the binary signatures of known malware. At worst, antivirus protection lures you into a false sense of security. You are protected against known viruses, but a new one might hit your device before an antidote has been developed...”

Steven Lentz, Director of Information Security at Samsung Research America, told the outlet that “defense in depth” is crucial because of the deficiencies of traditional antivirus. He called for features such as: application-based malware coverage and zero-day malware firewall protection for mobile devices.

Mobile Weak Spots

Put quite frankly: Mobile devices demand diligence at the CISO level. In fact, like the mobile device’s counterpart, workstations and laptops, many loaded malware campaigns begin with phishing attempts. (As mentioned earlier, the mobile breach could allow for expansive lateral movement.)

In a previous report for the Cyber Security Hub, the site wrote: “Phishing campaigns tend to be mobile mainstays – they capitalize on human gullibility and can inflict serious damage on various endpoints once firmly planted.”

Doug Cahill, Senior Analyst with ESG Global Research, told the Cyber Security Hub at the time: “On phishing, I feel like we’ve been seeing the same movie for a few years now. Adversaries typically prey on human gullibility – on users that operate endpoint devices.”

The key here is post-phish, however. Telecom Asia reporting also united some of the most utilized mobile attack methods. These included public Wi-Fi exploits, phishing attacks, MATM attacks, vulnerable OS compromise, modified settings exploit and root/jailbreak exploit.

Weaknesses in these areas of the mobile device, or persistent black-hat effort, ultimately perpetuate mobile infection – be it with malware from a suspicious mobile URL or a compromised app.

In a recent piece, Information Age’s Aaron Hurst wrote about a number of mobile weaknesses, and the usual suspects in mobile infection. One of those methods was drive-by downloads. The drive-by consists of a piece of malware hidden within a website that appears innocuous. The hope is that a weakness in the user’s computer or device will allow for a click and subsequent infection. To do this, hackers typically use exploit kits that sniff out vulnerable websites. Once the site gets the go-ahead by an unsuspecting visitor, the malware is downloaded on the user’s device. It then contacts another computer to initiate further coding to access the device.

Shoring Up Mobile Defense

For a previous report, Randall Frietzsche, CISO, Denver Health, told the Cyber Security Hub that with mobile devices, “We must make sure we are in control of (them). If you’re not in control of (a device) and it connects, the risk becomes quite high.”

But what are some best practices that professionals can adhere to? Frietzsche suggested they expertly vet the device and the data it holds. To think like a hacker, a CISO might need to understand the closest jump-off points to critical resources.

Frietzsche suggested CISOs “limit as much as you can (and) isolate it so it can’t compromise your network.” He also pointed back to risk management principles and questioning whether network connectivity is something that is warranted. Can the network handle the mobile device or should the takeover threat overpower that urge?

For this report, CDM Smith Principal, Director of Global Information Security, Jim Livermore, told the Cyber Security Hub that measures that can help mitigate the risk of mobile malware include MDM tools, implementation of MFA and deploying behavioral monitoring of the devices.

“Also, access on mobile phones to corporate applications should be through a separate secured partition and access to the corporate network should be segregated from the internal network,” Livermore said. “Finally, (useful tips include) providing user awareness training to ensure effective password management, identifying phishing emails and downloading suspect applications from official app stores.”

Security expert and Virus Bulletin Editor, Martijn Grooten, told the Cyber Security Hub that “anecdotally, most malware targeting enterprises still uses desktops and servers to enter the network, but data stolen through mobile malware ends up being for sale in the criminal underground and thus this forms a real risk. For protection (then), mobile devices benefit from relatively well-vetted app stores. The enforcement, especially on Android, of only using the official app store, prevention of rooting the device and the use of a third party antivirus product help even more.”

Microcosm Of The Threat Landscape

While it’s tough to predict what the exact future of enterprise mobility (and its security, in particular) looks like, it will certainly ebb and flow with the wider threat landscape, so the same attack mechanisms plaguing computers and laptops.

Helping us determine what the mobile security space could look like, and specifically contention around malware, we spoke with CDM Smith’s Livermore. The security expert said, “Hackers view mobile devices as an effective attack vector to gain unauthorized access to applications and data. As such, they will continue to refine their approach.”

He pointed to ad and click fraud as a “growing concern”; here, hackers compromise advertisements on mobile devices and bait users into clicking ads of interest. Then, unknowingly, they’re deploying spyware and malware on the device.

“Hackers can also create malicious apps that look legitimate and have them approved for download in the phone’s app stores,” Livermore added. “Users then download them thinking they are good apps and in turn download malicious code to their phones.”

The CDM Smith executive added that mobile botnets continue to be a threat – and can result in wide-scale control of an infected device. So, awareness around botnet threats is warranted.

In closing, mobile security is a profound domain in and off itself. Of course it fits neatly into wider security efforts, but it is clear that CISOs and security experts alike are focusing their attention on bolstering endpoint defense, and researching ways in which today’s threat actors are exploiting them. This dynamic, it seems, will prevail.
Information is at the core of every business. Data is valuable, whether it relates to a company’s business strategy, its competition or its customers. And with network environments that are increasingly interwoven and physically dispersed, safeguarding corporate data is harder than ever. Cybersecurity risks have multiplied with the spread of mobile computing and the Internet of Things (IoT). And the business cost of a breach can be catastrophic, in real financial terms as well as in reputational damage.

This situation has led to a new class of managed security services, which combine security operations centers, threat detection technology, endpoint management and human expertise. It’s a broad and complex area, which can include everything from identity management to vulnerability assessments, from endpoint management to enterprise firewalls. Managed CyberSecurity Services from AT&T can cover all the bases, with a robust portfolio of offerings that can be customized for the needs of individual companies.
ABOUT CYBER SECURITY HUB

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure their enterprise.

We’re dedicated to providing the latest industry news, thought leadership, and analysis in the cyber security space. Cyber Security Hub’s expert commentary, tools, and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

CYBER SECURITY HUB

Dorene Rettas
Managing Director, Cyber Security Hub
Enterprise Mobility Exchange
Dorene.Rettas@CSHub.com

Dan Gunderman
Editor, Cyber Security Hub
Dan.Gunderman@CSHub.com

Michael Roberts
Sales Director, Cyber Security Hub
Mike.Roberts@CSHub.com

Jodi Lozauskas
Marketing Manager,
Cyber Security Hub
JodiL@CSHub.com

UPCOMING MARKET REPORTS

OCTOBER: Beyond The Firewall: Breaking Down Layered Security
NOVEMBER: Cyber Security Challenges, Focuses For 2019
DECEMBER: Proactive Vs. Reactive: How To Monitor The Threat Landscape

SOCIAL MEDIA INFORMATION:

Twitter: CSHubUSA
Facebook: CSHubIQPC
LinkedIn: Cyber Security Hub - Enterprise Security Professionals