FIVE MOBILE SECURITY MYTHS DEBUNKED

Securing enterprise smartphones and tablets against cybercriminals is serious business. Unfortunately, even seasoned security professionals believe common misconceptions about keeping devices protected.

There used to be a time when companies did not need to worry about mobile devices. Today mobile devices may be the weakest security link in the enterprise. A 2017 survey of IT security professionals showed 20% of companies had a mobile security breach. A quarter of respondents did not even know whether they had experienced an attack. Yet nearly all expected the frequency of mobile attacks to increase.[1]

With approximately 80% of organizations adopting Bring Your Own Device (BYOD) programs to increase efficiency, this comes with a considerable amount of risk.[2] In fact, a recent survey of more than 850 global businesses determined that each business experienced at least one mobile malware attack in the past year.[3]

A single compromised device can allow cybercriminals to spy on closed-door meetings by using its microphone and camera. As an unwitting employee uses their compromised device and logs into corporate systems containing sensitive data, cybercriminals 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.

[1] The Growing Threat of Mobile Device Security Breaches, Dimensional Research, April 2017
[2] 2016 BYOD and Mobile Security Report (by Crowd Research Partners)
[3] Mobile Cyberattacks Impact Every Business, Check Point Software Technologies, October 2017

This paper identifies the five most common misconceptions about mobile security and how you can secure your mobile workforce.

1 MOBILE ISN'T A BIG PROBLEM

Firewalls and security infrastructures that protects PC desktops and laptops does not provide enough protection from *mobile* attacks. In a survey of more than 800 global cybersecurity professionals, only 30% of organizations increased their security budgets in 2016 to cover mobile devices, despite at least one in five organizations experiencing a mobile security breach the previous year. Of these, 39% downloaded mobile malware and 24% connected to a malicious Wi-Fi® network.[4] If mobile security is not a top priority for your company, it should be now.

Banks understand the threat and are more likely to invest in mobile security. When asked to identify their top five challenges, 60% of bank CIOs said "Keeping up with security issues."[5] While a live bank robbery may occur two to three times a year and cost around $10,000, bank cyberattacks sometimes occur 20-30 times *per hour,* and can cause over $50 million in damages.[6] Just one successful cyberattack can cause a disproportionate amount of damage and they may never be caught.

Mobile attacks come from three primary sources: network attacks, infected apps, and system exploits. While testing mobile security for prospective customers, Check Point regularly finds five to 20 percent of enterprise devices are already compromised. It takes only *one* compromised device to penetrate your security perimeter.

Discovering a breach takes an average of about 146 days globally and approximately 469 days in the EMEA region. [7] This means that once a breach is detected, the damage is already done. Remediation can be costly, as is containing the damage to brand reputation. Even if the damage is under control, your company may not know vital trade secrets were compromised until your competitive advantage is suddenly lost.

[4] 2016 BYOD and Mobile Security Report, Crowd Research Partners. In the one out of five breaches, 39% were from downloaded mobile malware, and 24% were from malicious Wi-Fi networks.
[5] "Banks to spend more on tech in 2016 – Especially Security," American Banker, Oct. 15, 2015.
[6] "Check Point CEO Talks Need for Prevention to Battle Crime" in InfoSecurity Magazine, Apr. 19, 2016.
[7] Breach Detections by the Numbers: Days, Weeks or Years? In Infocyte, July 2016

2 MDM IS ENOUGH

Many companies rely on basic mobile hygiene policies using mobile device management (MDM) or enterprise mobility management (EMM) solutions. Some augment these solutions with a hodgepodge of point solutions that offer incremental and often rudimentary enhancements.

These solutions help control damage inflicted by compromised devices and address many known threats, but are unable to detect recently created malware or new vulnerabilities in networks, operating systems, and apps.

For example, gaining root access to a mobile device (also called "rooting" on Android or "jailbreaking" on iOS) enables cybercriminals to make a broad range of customizations and configurations to serve their objectives. MDM and EMM systems detect the existence of certain files in a system directory that enable root access by employing several methods, including *static* root indicators. However, free tools for Android and iOS devices are available for avoiding this type of detection. By changing root access indicators continually, cybercriminals can evade detection, and even deny root check requests from the EMM or MDM system, disabling detection entirely.

Even high-tech companies that develop core security technology are not immune. Samsung Research America (SRA) recognized the potential security threat to sensitive information on its own mobile devices. SRA enlisted Check Point to test 1,200 mobile devices, 400 of which were employees' personal devices. Five percent — roughly 60 devices — in SRA's R&D department were infected with malware such as credential stealers, keyloggers, remote-access Trojans, and unauthorized root kits.[8]

MDM and EMM static root indicators cannot identify all of today's ever-changing threats. Security infrastructure for corporate PCs and laptops isn't enough either since mobile devices work beyond the network, creating potential security issues and enabling malware to enter.

[8] Samsung Research America Secures Intellectual Property from Advanced Mobile Threats, Check Point, 2016.

3 SECURE CONTAINERS ARE SAFE

Secure containers for data management platforms provide security *inside* the enterprise perimeter. However, mobile devices often access systems and apps like Salesforce, Oracle, or SAP *outside* the perimeter. While these systems and apps have their own protections, network spoofs or man-in-the-middle attacks eavesdrop, intercept, and alter traffic. Everything a user does, including entering passwords, could be intercepted by criminals, and used to breach the perimeter and to steal financial and personnel information.

Attackers often trick employees into logging into malicious sites. While users believe they are interacting with a known and trusted entity in the cloud, the attacker takes over their device, copying credentials, snooping on instant messages, or stealing their sensitive information.

For example, conveniently accessible public Wi-Fi hotspots are easy to fake. An attacker creates a spoofed Wi-Fi network, or eavesdrops and alters a legitimate network's encrypted communications. Using spoofed certificates or downgrading the communication link, the attacker decrypts the communications. Then, they intercept all communications, altering data in transit, and can remotely install a Trojan onto a mobile device.

Corporate executives and employees sometimes save critical documents and sensitive information *outside* the secure container – using a cloud storage service to easily access while travelling or share with partners. Once compromised, attackers intercept these communications and access these important and sometimes confidential documents.

4 IOS IS IMMUNE

Apple's iOS is not immune to threats. Some organizations using MDMs unwittingly distribute infected apps to iPhones and iPads. Apps from unauthorized, unreliable app stores may also harbor viruses, and hackers even compromised Apple's development tools, sneaking malware into new apps without the developers' knowledge.

Check Point recently discovered a vulnerability found in iOS that exploits a loophole in the Apple Developer Enterprise program. The program lets organizations develop and distribute apps for internal enterprise use without publishing them on Apple's App Store. These apps typically distribute quickly and directly to devices.

However, malicious apps can use this same method and enable criminals to stage man-in-the-middle attacks and hijack communications between managed iOS devices and MDM solutions. This type of exploit gives criminals control of the devices, the data that resides on them, and even enterprise MDM services. This exploit potentially impacts millions of iOS users worldwide whose devices are managed by an MDM.[9]

iPhone and iPad users mostly download apps from the highly secure Apple App Store. But still, many download apps from less reliable *unauthorized* app stores that harbor malicious code. These unofficial stores are on rise, and often see downloads of up to eight million apps a day.[10] Several third-party app stores abuse the enterprise distribution method by registrering for the Apple Developer Enterprise program and obtaining an enterprise certificate. With this certificate, they install apps on their customers' devices.

While Apple's review process for apps in the App Store is stringent and comprehensive, some apps on the store are vulnerable. When hackers could not get through Apple's review process, they modified the development tool. XcodeGhost, a compromised version of the Xcode developer platform for iOS, silently slips malicious code into apps in an undetectable way. Over 39 infected apps were found in the App Store as a result of XcodeGhost.[11]

Flaws in Apple's enterprise app installation process allow the introduction of unverified code into the iOS ecosystem. MDM systems could end up being the distribution systems for the very malicious apps they are defending against. Without an advanced mobile threat detection and mitigation solution on your iPhone, you may never suspect that any malicious behavior ever took place.

[9] "Bypassing the iOS Gatekeeper," Check Point, 2016.
[10] Over 40 million users download eight million unauthorized apps each day from stores such as 25pp, and vShare offers more than 15,000 unauthorized iOS apps.
[11] "How malware finally infected Apple iOS apps: XCodeGhost" on ZDNet.com, Sept. 20, 2015, and "Hackers Sneak Malware into Apple App Store," Forbes, Sept. 18, 2015.

> DEFENSE IN DEPTH IS NEEDED BECAUSE TRADITIONAL ANTIVIRUS IS NOT ENOUGH FOR ADVANCED THREATS.
>
> **Steve Lentz**
> CSO and Director of Information Security
> Samsung Research America

5 MOBILE ANTIVIRUS IS ALL I NEED

Many companies rely on antivirus products for PCs and laptops. These products employ advanced detection techniques because PCs and laptops have sufficient CPU power and memory, and battery life is not an issue. However, that is not the case with antivirus products for mobile devices. They cannot use the same advanced detection techniques 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, criminals have found new ways to obfuscate those signatures, making them useless in the detection mobile malware. Even a slight change in the code, such as adding a simple line that does nothing, changes the app's signature and the new version of the malicious app will slip by undetected by the antivirus program.

Signatures are not available for "zero-day" (newly created) malware. To catch and block a virus, your antivirus program first must know that it exists. Check Point uncovers new malware and attacks *constantly.* Even if updated daily, antivirus programs still couldn't keep up with the onslaught of these attacks.

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. "Defense in depth is needed because traditional antivirus is not enough for advanced threats," noted Steven Lentz, Director Information Security at Samsung Research America. "We need multiple layers of protection and critical features like application-based malware coverage, enterprise integration, and zero-day malware firewall protection for mobile devices."

CONCLUSION

Mobile devices require a new, intelligent approach to threat prevention. MDM and EMM protection and secure containers are not enough, and antivirus products cannot cope with new malware found every day. Even iPhones are not secure. The continuous, rising wave of attacks puts your company at serious risk.

You need a solution that continuously analyzes devices, uncovering vulnerabilities and criminal behavior. Check Point offers an intelligent approach to mobile security that detects and prevents both known *and unknown* threats — by applying threat emulation, advanced static code analysis, app reputation, and machine learning.

Check Point SandBlast Mobile analyzes behavior across *all* vectors for indicators of attacks. Integrating with existing security investments, it supports incident response and provides continuous protection. By using a unique cloud-based Behavioral Risk Engine, it performs an in-depth threat analysis. The risk engine identifies suspicious patterns and behaviors over time, sandboxing apps in an emulator and seeing what they do before you install them.

Stop malware before it communicates with criminal servers, and detect threats at the device, app, and network levels. Always have an accurate picture of the threats devices on your network face and detailed information about how risk mitigation. With SandBlast Mobile, your network and mobile devices are protected.

Check Point
SOFTWARE TECHNOLOGIES LTD

LEARN MORE
Demystifying Mobile Attacks

LEARN MORE
How SandBlast Mobile Works

CONTACT US

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233
checkpoint.com