WHITEPAPER

# Mobile Security: The Single Biggest Cyber Vulnerability

*Why Mobile Threat Defense is critical to protect consumers and enterprise users today*

Published by

ZIMPERIUM®
MOBILE THREAT DEFENSE

MOBILE WORLD LIVE

# Introduction

Most of you reading this are using a smartphone or tablet to do your work because your organization has adopted a BYO policy or has provided a corporate device. You may do some of that work at a local coffee shop, and you may also download some fun games on that same device. It's also likely that you didn't jump on downloading that recent OS update that came through. Boom. When you next access your organization's network, there's a 60% chance that you will directly bring in a vulnerable device without even knowing[1]. When you do, all of your organization's best laid security plans will be for nothing.

We've come a long way. In just over two decades, the mobile device has evolved into a high-powered mini computer. The feature-rich smartphones, tablets and phablets we carry around with us today are a thousand times more powerful than the first PCs, yet organizations haven't added suitable security precautions to these new computers/devices of choice.

Nearly three-quarters[2] (72%) of organizations allow at least some members of staff to use their personal device at work today. For those that do, improved employee mobility (61%), greater staff satisfaction (56%) and increased productivity (55%) are just some of the benefits. But with these new benefits come new risks.

# New Risks

Smart devices have become an essential business tool – witness the unstoppable rise of BYOD – and the focal point of our digital lives. But as such, they have also come to represent a major target for malicious third parties keen to access on-board data and use them to leapfrog into critical enterprise systems. Smartphones represent a massive blind spot for IT leaders because they're able to circumvent traditional security controls. And hackers know this. The number of smartphone attacks recorded between January and July 2016 nearly doubled compared with the last six months of 2015. And smartphones accounted for 78% of all mobile network infections[3].

There are three primary challenges to the mobile ecosystem - devices, networks and apps:

## DEVICES

Their hybrid use for both personal and corporate scenarios can mean that some traditional security measures are unsuitable and employees will resist "security by surveillance" for privacy reasons.

Plus, they depend on the user updating to the latest Operating System (which includes security fixes). This should be done in a timely manner but is often neglected.

## NETWORK

Mobile devices are constantly on the move. Employees typically connect to Wi-Fi networks at home, at the coffee shop, at airports, on trains, etc. There is also the threat of auto-connecting to unmanaged and unsecured cellular and Wi-Fi networks.

## APPS

The volatility and vulnerability of app ecosystems make traditional security measures difficult to enforce and introduce extra risk into the enterprise. In fact, 90% of 126 mobile health and finance apps tested from the US, UK, Germany and Japan, were found to contain at least two critical security vulnerabilities [4].


# Mobile: Your Biggest Security Blind Spot

The very power, ubiquity and capacity of smart devices represent a security risk many organizations haven't yet fully appreciated. They store critical personal and corporate data and can provide access to even more sensitive data on the corporate network.

The risks are real. One in five organizations claim to have suffered[5] a mobile security breach, mainly due to malware and malicious Wi-Fi. And an even larger number (37%) said they aren't sure – highlighting the critical lack of visibility hampering security efforts today.

Organizations have a major problem: they don't have the visibility they need to understand where the main vulnerabilities, threats and risks lie in their mobile estate. Many are flying blind, unaware of the risks and unable to defend against attacks. Zimperium conducted a risk and live threat assessment[6] for a typical US company over a four-month period. **After installing Zimperium Mobile Threat Protection on 7000 devices, 60% were found to be vulnerable.**

Things will only get worse. Gartner claims that by 2018, a quarter of corporate data traffic will flow directly from mobiles to the cloud, bypassing any enterprise security completely.

Some enterprises receive this protection through innovative mobile operators looking to protect them and offering these value added services.

It's a new breed of security solutions which Gartner calls Mobile Threat Defense (MTD).

# No Immune System

The most vulnerable computers that access your systems today are mobile phones and tablets. But many IT teams aren't aware because there are no on-board sensors detecting threats. It's like a body without an immune system. It can't defend itself or self-repair once under attack.

But we can't simply transfer our desktop-based security tools and techniques into the mobile world. Consider how your organization secures its network and information from unauthorized access via mobiles.

There are specific and unique challenges which make mobile different. They include:

**Real-time:** Sophisticated machine-learning techniques are required to assess risk real time, and perform on-device detection of threats.

**Unknown threats:** Previously unseen threats capitalize on new vulnerabilities in mobile operating systems. MTD solutions provide zero-day detection of these unknown threats on the device or minimally by cloud-based analysis.

**No root privileges:** Traditional security solutions have administrative and root privileges to detect and stop threats. These will not work in the mobile OS world.

**Resource limitations:** Unlike traditional security environments, mobile devices have limited resources, from battery lives to network bandwidth. MTD solutions are designed to minimize the impact on these valuable resources.

**Host based attacks:** Cyber threats such as malware, can be targeted at specific devices, including forms of spyware, adware, ransomware and can access personal information on the device as well as company information. A malware infected device can act as a jumping off point once connected to a company intranet, further infecting servers and desktops in the environment. Traditional security tools simply can't detect these attacks.

**Network attacks:** Mobility puts smartphones and tablets at risk. They're often used to connect via highly risky public Wi-Fi networks in airports, hotels, coffee shops and the like. Rogue Access Points are wireless networks that purport to be a legitimate Wi-Fi network. These "rogue" networks often have the same name as well known public Wi-Fi networks and need proactive detection to see a compromised network or active attack.

**Devices:** The sheer heterogeneity of the mobile universe makes it difficult to enforce security policies across the board and find the right tools to support all of your employee's devices.

When it comes to Android, there are a huge range of architectures, OS versions, vendors and settings to consider. The infamous Stagefright vulnerability impacted nearly every Android device in the world. And many thought iOS was immune from similar remote attacks until Pegasus appeared. This spyware package existed for over two years before it was found attempting to transform a device into a remotely controlled surveillance tool for tracking a person, reading data and listening to conversations.

**User experience:** Smartphones can be your employees' biggest productivity tool. But that means any security solution must be completely un-intrusive to the end user or could lead to additional IT security risks if users attempt to bypass controls.

**Privacy:** Many security solutions send device and usage data to the cloud for analysis. But that has drawn strong criticism from end users who are demanding their privacy rights be respected – especially if they are using a personal device for work.


# Threats and Impact

As we've described, the mobile threat to organizations is real. Zimperium's Global Threat Intelligence research on a US company yielded the following additional insight:

- Network threats were 15 times more common than application threats
- 6.2% of devices recorded a critical threat event including traffic tampering, man-in-the-middle attacks, and a rogue access point
- 5% of the analyzed devices recorded a reconnaissance scan – an intermediate level threat which typically precedes a more serious network attack
- Around 1% of devices had been infected by malicious apps

Remember: even threats in the low percentages could have serious repercussions. It takes just one compromised device for hackers to access the corporate network. The impact of such a data breach and/or malware infection could be devastating.

In 2016, the average cost of a total data breach stood at $4m[11], up almost a third (29%) from 2013. Some of the potential cost impacts of a mobile security incident include investigation, remediation, and legal and regulatory fees. In addition are the PR cost of brand damage; share price slump; increased IT/helpdesk workload; and, importantly, loss of customers.

## Two Major New Threats

Gooligan[12] is a new Android-based malware family which has compromised over one million Gmail accounts, some of them corporate. It's hidden in legitimate looking apps in third party app stores but is also spread through malicious links in phishing messages. If successful it will root the device, giving attackers full control. *This was detected real time by Zimperium.*

Pegasus[13] is a device-level iOS trojan leveraging three zero-day bugs to remotely spy on a targeted device. Infection comes via an innocuous looking link, and with this kernel-level exploit an attacker gains complete visibility into the device's communications, including calls, texts, WhatsApps etc. Its sophistication led many to believe it was commissioned by a nation state. *This was detected real time by Zimperium.*

# Time for Mobile Threat Defense

Without Mobile Threat Defense in place, the average time for an organization to identify a malicious attack on its network stands at 229 days[14]. And it typically takes another 82 days to contain the threat. It's no surprise that mobile device infections soared 96% in the first six months of 2016[15], as cybercriminals grew increasingly adept at circumventing current security filters.

So, what's wrong with legacy mobile security tools?

**Network security** products can protect mobile devices from attacks on the corporate network, but have no visibility once they leave the network - which is often.

**Mobile AV** will block malicious apps by scanning for signatures, but it can't protect against unknown malware or zero day threats.

**Mobile Device Management (MDM)** solutions focus on preventing non-compliant devices connecting to the network, incorporating features like device wipe. But they can't protect against actual cyberattacks.

**Mobile Application Management (MAM)** products take a "containerization" approach, which effectively involves sandboxing to mitigate possible threats. But it is complex to roll-out, disruptive for the end user and can be circumvented by, for example, kernel exploits.

## A NEW APPROACH

The only way enterprises can be confident that they understand the risks facing their mobile estate and can deal effectively with the threat, is by taking a new approach optimized for the mobile-centric world. Security must be always on, detecting threat activity round-the-clock even when not connected. And it needs to do this without impacting the user's experience or privacy. This is Mobile Threat Defense.

By leveraging the power of machine learning, cutting edge MTD tools can distinguish 'normal' from 'malicious' behavior. Thus, by analyzing minute changes to things like memory, CPU and OS data they can identify and block the specific threat and provide vital forensic data on the who, what, where and how of an attack. Crucially, this approach means they're able to spot new and unknown zero day threats in real time - no updates required.

By downloading highly developed MTD sensors/apps on all mobile devices, organizations can build their own immune and early warning system to block threats; gain visibility into attacks; and remediate where appropriate.

Here's a quick checklist of features to look for:

- Behavior-based machine learning protection of abnormal activity on mobile device
- Protection against host and network attacks to prevent infected devices coming back onto the network
- Immune to evasion techniques – known and unknown threat detection
- Always-on, real time on-device detection – doesn't need to be connected, won't drain battery
- Platform agnostic – works across iOS and Android
- Integrates with MDM / MAM solutions
- Solution designed specifically for the mobile environment

In the past year alone, the number of mobile threats facing organizations and consumers has exploded as hackers realize how effective they can be. The table below lists some of the named threats and highlights how MTD (with Zimperium's z9 detection engine using patented, machine-learning algorithms,) detected every one in real time[16] .

| Exploit/Attack | Type | z9 Detection Status |
|---|---|---|
| Dirty COW | Local | Successful Dirty COW Attacks: z9 detected without an update.<br><br>Unsuccessful exploit attempts: We created new z9 simulation to provide an alert as well. |
| Ian Beer's iOS 10.1.1 | Local | Detected without an update |
| Gooligan | Local | Detected without an update – just a reuse of TowelRoot and VRoot in apps, mostly of third party marketstores - z9 doesn't need to have app's signatures to detect exploits. |
| Pegasus | Remote | Detected without an update |
| Stagefright | Remote | Using our previous trainings of z9 for CVE-2015-1538 and CVE-2015-3864 z9. Google Project Zero Stagefright exploit CVE-2016-3861: detected without an update. |

What's important to remember, however, is that these threats didn't always have an official name, marketing campaign or associated documentation. It's another reason why machine learning MTD can spot hitherto unknown threats in real time, without needing to update its detection engine. Once the information exists to update the engine, the threat is less likely to be used by black hats anyway. Plus, it's in those key days, weeks and months, before it has been officially recognized, that matter.

## Danger at the airport

A Zimperium employee passing through Dallas Fort Worth airport recently avoided a Man in the Middle attack thanks to Mobile Threat Defense on his device. The smartphone in question automatically connected to a known public Wi-Fi network in the airport. A short time later the on-device MTD detected a scan, and soon after detected a network hand-off. Like the body's immune system, MTD determined from the device's behavior that it was suffering a critical MITM attack. Within 120 seconds of the handset first connecting to Wi-Fi, MTD disconnected and alerted the user.

# Operators: Mobile Security is a Win-Win

Much of our discussion of mobile threats and their impact has been focused on the corporate sphere. But make no mistake, mobile security has major implications for the operator community – both in a B2B and a B2C context.

As we've shown, the threats are universal. Both consumers and employees are at risk from a growing variety of cyberattacks targeting smartphones, tablets and other smart devices.

Mobile Threat Defense therefore represents an opportunity for operators on two fronts, both of which increase stickiness and customer lifetime value:

1) Offer MTD tools to corporate clients to help them reap the productivity benefits of BYOD whilst solving the associated security challenges at device, network and app layers.

2) Offer MTD to consumer subscribers as a value add which will help differentiate the brand on security in an increasingly crowded marketplace.

# IoT - Just More Mobile Connected Devices

Crucially, IoT devices can be hacked exactly the same way as smartphones and tablets. And again, they bring vulnerabilities back into the corporate network.

That's why enterprises and operators must bring them under the auspices of their mobile security programs. For mobile operators looking to add value in a growing smart home and connected life space, it's an opportunity to differentiate on security. And for enterprise CIOs, it's a fundamental necessity to secure all potentially risky new mobile devices appearing in the workplace.

# Time to Call Security

It's time to get nervous about the vulnerabilities of mobile devices and serious about mobile threat defense.

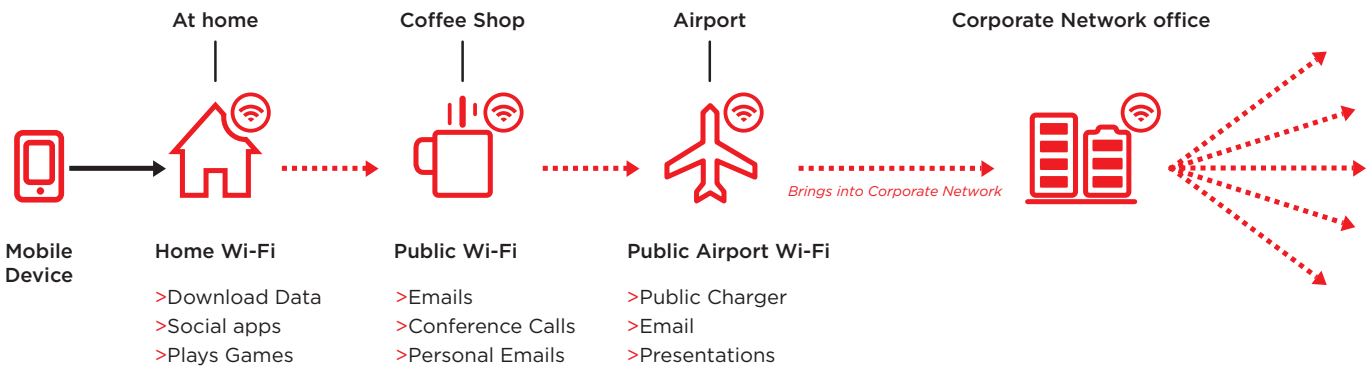
Organizations face a major challenge in gaining visibility into their mobile estate and developing the kind of "immune system" which will help defend against the growing variety and volume of threats targeting the mobile ecosystem.

Many firms have spent millions establishing security at the network perimeter, installing best-of-breed firewalls, Deep Packet Inspection tools, web and email gateways, and more. But that means when hackers manage to penetrate the hard outer shell of this "jelly bean" security they meet with relatively little resistance inside.

And mobile is the ideal vector for them to burst through, potentially offering a direct path into the network and all the highly sensitive data stored on corporate servers.

Here are some of the key questions enterprise IT leaders and executives in operator organizations should be asking security teams:

- Do we know what constitutes an acceptable level of risk on mobile devices and can we enforce it?
- Do we know if threats are being targeted at our employees' mobile devices today?
- Do we have on-device behavior-based security tools designed to protect against all host and network attacks?
- Do we know what type of vulnerabilities we are introducing our customers to via our mobile apps?



[1] Zimperium, 5 Facts Every Executive Should Know About Mobile Security
[2] Crowd Research Partners, BYOD & Mobile Security Report 2016
[3] Nokia, Nokia Threat Intelligence Report – H1 2016
[4] Arxan, 5th Annual State of Application Security Report
[5] Crowd Research Partners, BYOD & Mobile Security Report 2016
[6] Zimperium, 5 Facts Every Executive Should Know About Mobile Security
[7] ITbusiness.ca, IDC's 2016 Predictions: IoT Headed for Huge Growth (and Security Headaches)
[8] CNN, Widespread attack takes down sites worldwide
[9] Softpedia, Tesla Model S Hacked to Start Without Key, Jan 22, 2015
[10] Crackberry, How your tea kettle could be a gateway for hackers, July 22, 2016
[11] IBM, 2016 Cost of Data Breach Study: Global Study
[12] Zimperium, Zimperium users are safe from Gooligan
[13] Zimperium, Understanding – "Pegasus" a Targeted Attack Remotely Infecting iOS Devices
[14] IBM, 2016 Cost of a Data Breach Study: Global Study
[15] Nokia, Nokia Threat Intelligence Report – H1 2016
[16] Zimperium, Detecting unknown threats time after time

MOBILE WORLD LIVE

Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money.

What's more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

**Find out more www.mobileworldlive.com**

ZIMPERIUM®
MOBILE THREAT DEFENSE

Zimperium® is the industry leader in Mobile Threat Defense with the world's largest deployment of mobile device sensors. Only Zimperium offers continuous, real-time, on-device protection against both known and unknown threats, enabling detection and remediation of attacks on three levels - devices, networks and applications.

Zimperium's patented z9™ machine-learning detection engine uses artificial intelligence to power zIPS™, the world's first mobile on-device Intrusion Prevention System app, and zIAP™, an embedded, In-App Protection SDK that delivers self-protecting iOS/Android apps, as well as comprehensive app risk analysis with z3A™.

Leaders across the mobile ecosystem partner with Zimperium, including mobile operators, device manufacturers, and leading Enterprise Mobility Management providers. Zimperium is backed by major investors Sierra Ventures, Samsung, Telstra, and Warburg Pincus. Learn more at www.zimperium.com.



**Visit www.zimperium.com for further information.**