5 Facts Every Executive Should Know About Mobile Security

ZIMPERIUM

The Case for Mobile Security

Today, employee mobility is critical for enterprise productivity. Mobile devices, the networks they use and apps have become critical success factors for organizations who want to reach and satisfy customers, collaborate more effectively with suppliers, and keep employees productive anytime and anywhere.

Do you realize this connectivity opens the door to a whole new category of security threats? Mobile devices and apps have shifted from personal tools to business tools and now store valuable data and access your most critical systems, making them coveted targets for cyberattacks into your organization.

That's why mobile device threat protection is essential to any mobile enterprise. Here's what you need to know:

1. Mobile Is Your Greatest Cyber Vulnerability

Why? Because you are likely not protecting mobile devices from cyber attacks.

Hackers continue to innovate as they target your organization and key personnel. They look for the path of least resistance to your most critical systems and data. Your desktops and servers may have cyber security technologies protecting them, but you likely have no equivalent support on mobile devices. Cyber attacks are shifting to mobile, and you must defend yourself.

"By 2018, 25% of corporate data traffic will flow directly from mobile devices to the cloud bypassing enterprise security controls." [1]

Desktops and servers are hard enough to protect. Mobile devices add new challenges, bypassing many of the security controls you have in place, including:

Devices:

- Their hybrid use for both corporate and personal matters
- Privacy issues that make traditional methodologies unsuitable for securing them

Network:

- Their ability to auto-connect to unmanaged and unsecured networks
- Their broad attack surface that includes every desktop attack vector, plus ones specific to mobile such as Wi-Fi, Bluetooth, NFC, charge ports, applications and more

Apps:

- Their volatile ecosystem that makes traditional security practices hard to enforce
- BYO Apps introduce unknowns into the enterprise

Today, you are most vulnerable to cybercrime via mobile devices. Very few organizations have visibility into mobile platforms to assess their vulnerabilities, identify threats and measure risks. Most cannot identify which devices are too risky to entitle with email and other enterprise system access. Most are unaware of which devices are running malware or frequently

connecting to malicious Wi-Fi hotspots. They do not know their risk, and they cannot defend against an attack.

2. The Mobile Threat is Real

Zimperium compiles mobile threat data across several geographies, industries and organizations. Here are the risk assessment and live threat detection results of a US-based company over a four-month period in 2016. Image 1 below represents the static risk of devices with a mobile threat detection application installed.

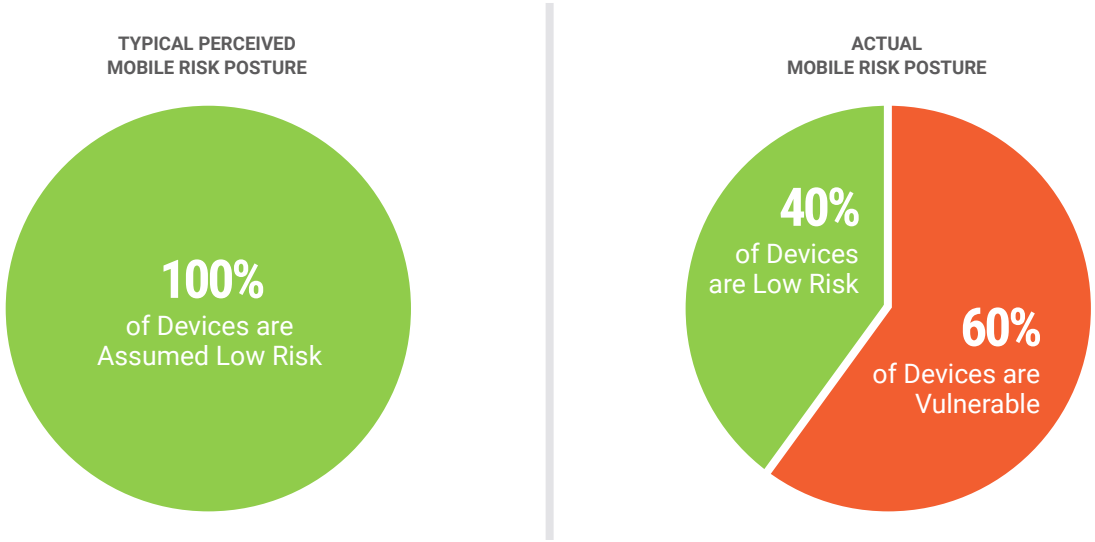

Image 1: Your Current View of Mobile Security[2]

After installing Zimperium Mobile Threat Protection on 7000 devices, this customer found:

- 60% of mobile devices were operating on outdated OS versions and highly vulnerable to known exploits.
- After remediation and resolution of issues, most devices became compliant. Still, at least 10% of these devices were deemed too high risk to entitle with corporate credentials.
- 6% of active devices remain vulnerable to one or more known vulnerabilities.
- Jailbroken or rooted devices active in the corporate environment constitute 0.5% of active devices.

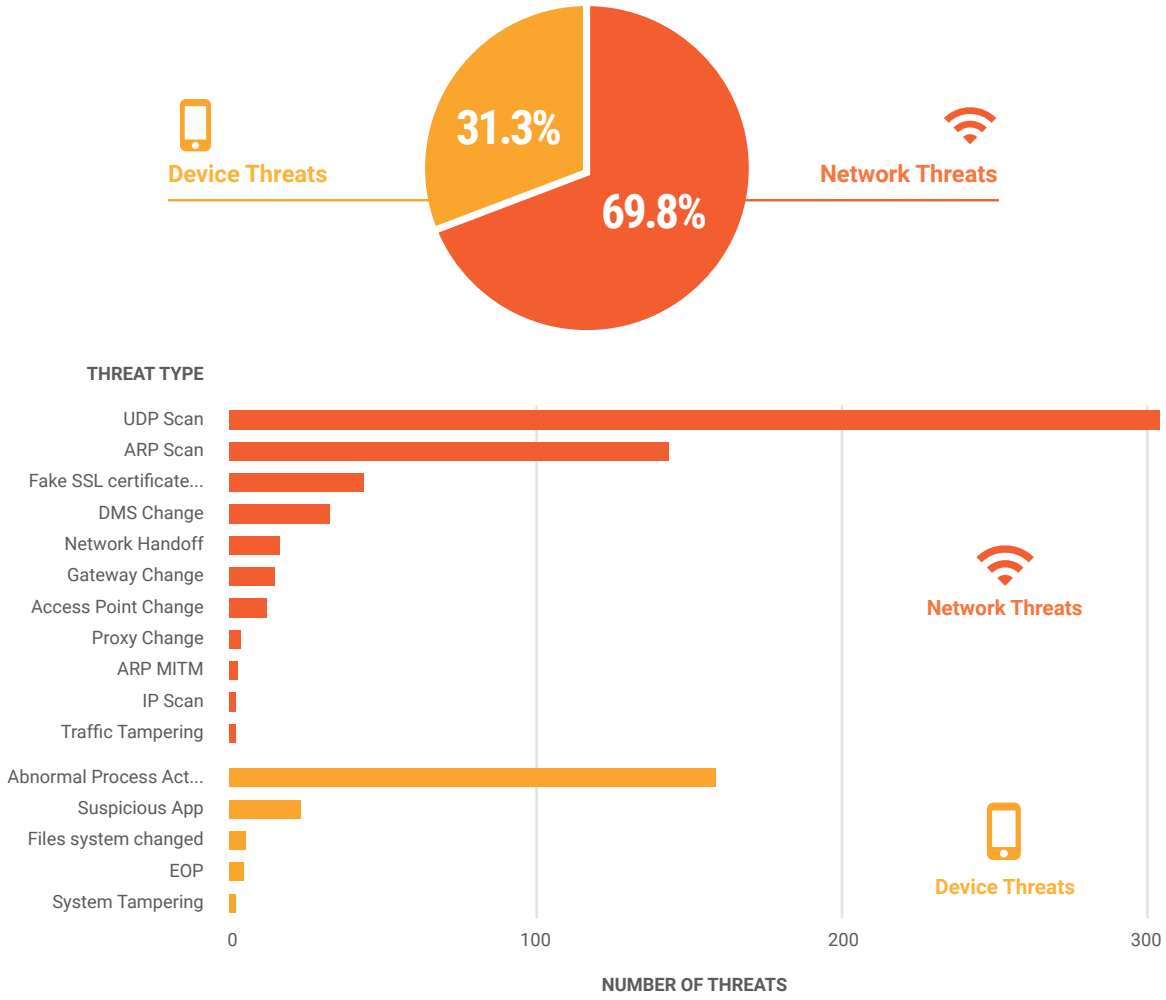

Image 2: Network vs. Device Threats [3]

Measuring and collecting threat data amongst this customer's devices found:

- Network threats were 15 times more common than application threats.
- Devices recording threat events in this period represented almost 70% of total active devices.
- 6.2% of devices recorded a critical threat event and provided correlating forensic data to the customer's enterprise security team. This environment recorded amongst their active devices traffic tampering, man-in-the-middle attacks, and a rogue access point.
- Five percent of the devices recorded a reconnaissance scan which is an intermediate level threat. Elevated scans of this type precede network attacks and cause the threat detection technology to correlate events.
- Consistent with other threat reports, approximately 1% of devices had been infected with malicious apps.
- Operating system privileges were obtained maliciously on 0.1% of devices.

A compromised mobile device can inflict devastating damage on an enterprise. Once weaponized outside a network, it can often wreak havoc within a company's premises without detection, and forensic analysis often cannot even identify that a mobile device was in use during the attack.

3. Mobile Threat Protection (MTP) Mitigates Business Risks and Threats

To assess the risk and remediate threats in real-time on mobile devices, a new class of software called Mobile Threat Protection (MTP) has been created. MTP is very different than traditional cyber security approaches.

Today's approach for mobile cybersecurity needs to be real time, proactive and must be coupled with the high expectation for privacy.

The traditional approach to protect desktops and servers could be characterized as security via surveillance. Employees have no expectation of privacy on their corporate desktop computer, so reading their web traffic and emails is not generally an issue; neither is preventing them from changing the administrator configuration of the desktop. None of this is feasible with hybrid-use mobile devices.

Your organization might have employed an Enterprise Mobile Management (EMM) solution, but it is not MTP. EMM is geared toward compliance of employee behavior, which is certainly an important facet of security, but completely insufficient for mobile threat detection. Ideally, you will have a MTP solution integrated with your EMM adding cybersecurity compliance policies and to extend its value for a complete mobile security defense.

Some might consider their containerization technology sufficient for MTP, but this is also inadequate. When a hacker compromises a device, the containers are compromised as well. The network and stored data is at risk, and live data (on screen, keyboard, or memory) is wide open for the taking.

For MTP to be successful, sophisticated machine-learning techniques are required to assess risk real time, and perform on-device detection of threats. This provides the greatest possible coverage, yet requires no private user information to leave the device.

Below is an abbreviated summary of the types of risk and threat vectors that a world-class MTP solution provides. Note the three categories, DNA, for Device, Network, and Apps.

- **Device:** Monitor for device-level compromise via exploit or risky configuration settings.
- **Network:** Wi-Fi and cellular networks can be compromised and thereby enable mobile attacks.
- **Apps:** Malicious apps can bypass protection mechanisms and steal sensitive corporate and personal data.

While malware apps are definitely an issue, they are only one of the ways that mobile devices are compromised. A suitable MTP must cover all three facets of mobile security.

4. Protect the Apps You Develop

Thus far, we have discussed the corporate security risk associated with mobility. To encompass the full security exposure of mobile, we need to consider the apps that companies are producing for their consumers and partners as well. According to Gartner, *"By 2020, 60% of digital businesses will suffer major service failures, due to the inability of IT security teams to manage digital risk."*[4]

Apps are being developed by teams that are frequently inadequately trained and inexperienced with delivering their app to potentially hostile actors. The functionality these apps provide can be weaponized against the user and more often the company providing the app. These apps are deployed into an unmanaged world where the app developer cannot qualify the risk of the device, hygiene of its network connection, or even detect the presence of known malicious apps already on the device

Hacked apps typically create time-consuming and annoying issues for users who must remedy fraudulent transactions, but the company behind the app bears the full burden of the financial cost and brand damage associated with the malicious act. Ultimately, the app producer is the victim of the user's mobile vulnerability.

Zimperium provides a MTP solution as a software development kit (SDK), enabling your developers to integrate threat detection into your own apps. The app becomes self-protecting, meaning that if malicious intent is discovered, it is remediated inside the app itself. It requires no additional action from the user, and the security team now has visibility into the threats delivered to their apps in the wild.

5. Closing the Mobile CyberSecurity Gap

The conversation you start now could go a long way toward reducing your organization's risks of mobile attacks. We recommend business leaders ask their security teams open-ended questions to begin the dialogue in their organizations regarding mobile risk:

- Have we adopted a position concerning the acceptable risk posture of mobile devices and can we enforce it?
- Do we know if threats are being perpetrated on our employees' mobile devices today?
- Have we performed an assessment of the potential security risks associated with our mobile apps?
- Have our security experts been involved in designing and developing the apps that we produce for our customers?

Zimperium's solution for enterprise mobile threat protection (MTP) is designed specifically for the mobile environment, and continuously delivers real-time protection against mobile device, network and application threats.

Through its disruptive, on-device detection engine using patented, machine-learning algorithms, Zimperium generates "self-protecting apps" that safeguard enterprises against the broadest array of attacks.

Zimperium integrates with leading EMM and containerization vendors. Contact us for a workshop on the many facets of mobile risk and threat and see how you can leverage our technology to close this critical gap.

Sources:

[1] Gartner, Special Report: Cybersecurity at the Speed of Digital Business, Paul E. Proctor, Ray Wagner, August 30, 2016

[2] Zimperium Global Threat Intelligence, 2016

[3] Zimperium Global Threat Intelligence, 2016

[4] Gartner, Special Report: Cybersecurity at the Speed of Digital Business, Paul E. Proctor, Ray Wagner, August 30, 2016

CONTACT US

101 Mission Street
San Francisco, CA 94105
Main: (1) 844.601.6760
info@zimperium.com

www.zimperium.com