Leaky Mobile Containers Pose Severe Risks to Email and Other Business Apps
Introduction

Prior to his murder in October 2018, journalist Jamal Khashoggi most likely believed the messages he sent from his smartphone to a fellow Saudi dissident were private and protected by WhatsApp security. Nothing was further from the truth, because his colleague’s device was compromised, infected by a sophisticated malware created to completely take-over and spy on mobile device users. No doubt, Khashoggi’s enemies were able to track his movements this way, and lie in wait for him in Istanbul, where he was killed.¹

In September 2019, a hacking group overtook Twitter CEO Jack Dorsey’s smartphone and proceeded to tweet racist posts from his account. It’s believed the hackers used a social engineering tactic to transfer a victim’s smartphone number onto a new phone, which the hackers owned, and began tweeting their vitriol.²

There is a common belief that implementing a Unified Endpoint Management (UEM) solution, or its predecessor, a Mobile Device Management (MDM) solution, with a mobile container provides solid protection for enterprise data. This is a misconception. Companies that build their mobile security strategy by relying solely on UEM and container technologies are exposing themselves to significant risks from cyberattacks.

Companies that build their mobile security strategy by relying solely on UEM and container technologies are exposing themselves to significant risks from cyberattacks.

In this paper we discuss and demonstrate how mobile containers are inherently insecure and incapable of protecting from mobile threats, and explain how organizations should implement effective mobile threat prevention using Mobile Threat Defense technology.
Containerizing Business Data

One of the most common approaches to securing sensitive corporate data – such as email and documents – has been the use of mobile device containers, which are frequently included with UEM (MDM) solutions. A mobile container is an encrypted area of a mobile device that can be used to store and isolate corporate data from the personal portion of the device. Containers rely on the operating system’s sandbox security model to keep data separate and secure, with each mobile application allocated its own separate storage space and permitted to perform only a specific set of functions. A mobile container will also allow IT administrators to remotely wipe a device in case it is lost or stolen.

While segregating business content on the device from personal apps is a good start towards enhanced control over corporate data accessed by mobile devices, this approach leaves a huge hole and creates a false sense of security.

Containers: The Inherent Problem of Operating in a Vacuum

Mobile containers are completely blind to threats and infections on the device. And as we all know, we cannot protect against what we cannot see. That said, it is difficult for threat actors to penetrate a fully-managed device, where all business information is containerized, because security administrators have visibility and control over the entire device. But what happens when a container operates in a split environment and can’t see both business and personal apps. And what happens when the personal, non-containerized portion of the device is infected?

Mobile containers are not designed to prevent attacks and infections on a device. Since the job of a container is focused on separating business and personal data, they provide zero visibility beyond the container. This means that by targeting the unsupervised side of the device – or the side in which personal apps and data reside – organizations can be attacked by malicious actors seeking to harvest user credentials used to access corporate email and sensitive data.
How Hackers Bypass Mobile Containers

Rootkits, or malware that exploits OS vulnerabilities, can access elevated privileges and attack the operating system itself. Bypassing all permission restrictions, malware can break the sandbox security model itself. Then the malware can bypass encryption software, as well as access storage, memory, and specific functionalities of any application. But hackers don’t always need to use sophisticated techniques to compromise sensitive information on a mobile device; sometimes a little social engineering can do the job.

Let’s see some examples of how sensitive information can get into the wrong hands, even with a mobile container:

- **Phishing**: Links to malicious sites are delivered through any one of the many messaging apps available on the device, including private or business email, SMS, WhatsApp, Telegram, etc. And because users are often distracted when using a mobile device, or simply less discerning because of its small screen, they are more easily fooled by phishing attacks. Malware can prompt a user for their credentials and steal them, gaining access to the container and any other sensitive data on the device.

- **Malicious Apps**: Keyloggers, for instance, which can be hidden in seemingly legitimate apps, can steal all the input of unsuspicious users, including credentials to the container and corporate apps.

- **Man-in-the-Middle Attacks**: Public Wi-Fi hotspots are easy to fake. An attacker may spoof a Wi-Fi network, or eavesdrop and alter a legitimate network’s encrypted communications. By using spoofed certificates, or downgrading the communication link, the attacker may decrypt communications. Then, they intercept all communications, altering or stealing data in transit.

- **Not All Business Happens Inside the Container**: A great deal of any user’s sensitive information resides outside the corporate container: contacts, pictures, location, SMS used for 2-factor-authentication, recordings of calls, calendars, etc. A malicious app could easily gain access to this information without rooting the device.
An Effective Approach to Mobile Security

Mobile containers do not provide the security required to protect mobile devices and the sensitive corporate data they contain. Neither do mobile management solutions alone. A complete mobile security approach requires UEM solutions to be integrated with a Mobile Threat Defense (MTD) solution. MTD solutions prevent attacks on iOS and Android devices by employing a variety of techniques, including machine learning and behavioral analysis based on mobile threat intelligence.

By gaining full visibility of the risk posture of mobile devices, admins can implement security policies that can be enforced in sync with their container and management solutions.

SandBlast Mobile: Unparalleled Threat Prevention

SandBlast Mobile is the market-leading mobile threat defense solution, preventing attacks from all mobile vectors. It detects vulnerabilities in the operating system, including advanced jailbreaking and rooting, and blocks malicious applications that can compromise the container and the data within it. In addition, SandBlast Mobile automatically disables the connection to networks when the device undergoes a Man-in-the-Middle or a bot tries to exfiltrate data to a command and control server, and prevents phishing attacks on any app.

With SandBlast Mobile, security professionals are always confident that corporate data inside or outside the container is protected.

For more information: www.checkpoint.com/mobilesecurity

1 CNN.COM, How a hacked phone may have led killers to Khashoggi
2 WIRED, How Twitter CEO Jack Dorsey’s Account Was Hacked

Read next: Mobile Management Solutions are Not Security