Five mobile security myths busted

By Doros Hadjizenonos

21 Oct 2016

Think your enterprise mobile devices are secure? Think again. The iOS and Android devices your employees use for work purposes are treasure troves of sensitive information, and it only takes one compromised device to put your business in a perilous predicament.

©kantver via 123RF

A 2014 survey of IT security professionals showed 75% of companies allow personal devices to connect to corporate networks. Workers use these same devices to download personal apps and emails – exposing your network to phishing scams and malware infections. More than one billion Android mobile devices are not safe – and may never be. iPhones and iPads aren't immune to risk either. In fact, there is a 50% chance that an organisation with more than 2,000 mobile devices has at least six infected devices.

Here are 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 protect PC desktops and laptops do not provide enough protection from mobile attacks. 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 5% to 20% 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 six months, and a response to fix the breach another three months. 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.

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 customisations 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.

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're 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.

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 organisations using MDMs unwittingly distribute infected apps to iPhones and iPads. Apps from unauthorised, unreliable app stores may also harbour 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 organisations 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.

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 behaviour ever took place.

5. Mobile antivirus is all I need

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 of 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. Even if updated daily, antivirus programs still couldn't keep up with the onslaught of these attacks.

Secure your mobile workforce

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 analyses devices, uncovering known and unknown vulnerabilities and criminal behaviour, by applying threat emulation, advanced static code analysis, app reputation, and machine learning. 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 and devices on your network and detailed information about risk mitigation.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...