Caldoo

Check Point
SOFTWARE TECHNOLOGIES LTD

A CISO'S GUIDE TO MOBILE THREAT DEFENSE

A CISO'S GUIDE TO MOBILE THREAT DEFENSE

You already know that cybercrime and espionage are on the rise, and that security breaches can cripple your organization and damage your brand and reputation. What you may not realize is that standard security solutions are not strong enough for mobile devices and apps in the workplace. This paper offers security professionals a better understanding of some of the unique challenges of securely enabling a mobile workforce.

OVERVIEW

The explosive proliferation of personal smartphones and tablets in the workplace exposes your company to increased risks. While a breach of personally identifiable information or payment card data is certainly a top concern for many businesses, there are other risks that any organization needs to consider. Chief among these are the cost of breaches and responding to incidents, the potential damage to brand reputation, and a loss of competitive advantage if valuable trade secrets or intellectual property become public knowledge.[1]

Mobile systems, the networks they connect to, and the apps they run can all be exploited to steal sensitive information such as documents, calendar appointments, email messages, texts, and attachments. Cyber criminals can use a device's microphone and camera to spy on closed-door meetings, and then send recordings to a secret remote server. They can even capture user names and passwords as users log in to corporate systems containing sensitive data. Unsecured networks, or networks using faulty or old security measures, make it possible for criminals to snoop, steal, or even change data sent to and from devices. Malicious apps can give attackers virtually unrestricted access to a device, its data, and your network.

Accurate threat detection and efficient response are critical components of preventing advanced attacks on smartphones and tablets. Traditional anti-virus and app reputation solutions can identify known threats, but they can't detect newly created malware or the vulnerabilities in networks, operating systems, and apps.

[1] The cost to understand and recover from a single breach soared 23% in 2015 to a breathtaking $3.79 million, according to the Ponemon Institute. Considering it takes an average of 256 days just to spot a breach and 82 days to respond to a breach, the damage happening without your knowledge could be catastrophic. In a survey conducted by Ponemon in April 2014, 29% said that a data breach made them less likely to have a relationship with the company, while 15% said they would discontinue their relationship altogether.

THE FIVE MAJOR THREATS TO MOBILE SECURITY

We've identified five major categories of attacks and vulnerabilities that can challenge the security of your business. For each category we include the best practices for dealing with these challenges.

1 SYSTEM VULNERABILITIES

Each version of an operating system for a mobile device offers vulnerabilities that cyber criminals can use to launch attacks. New versions are notoriously late to market. Critical security updates might not make it through testing for weeks or even months, leaving users exposed.

Android is particularly vulnerable. The 24,000+ different types of Android smartphones and tablets are not updated consistently and at the same time. Most devices are still using older Android versions in which vulnerabilities have not been patched.[2]

Apple's iOS is less vulnerable because Apple makes only a handful of different devices and consistently prompts users to update them.[3] However, though the number of attacks in 2015 was low, there were twice as many as in 2014, and these more sophisticated attacks work on devices that haven't been jailbroken.[4]

Cyber criminals make it their business to exploit the weakest links in your systems. You need a solution that continuously analyzes devices to uncover vulnerabilities and the behaviors cyber criminals use to attack devices. When a threat is identified, the solution must automatically mitigate any risk until the threat is eliminated. With better visibility into the vulnerabilities of mobile device systems, you can reduce your overall attack surface and your risk.

BEST PRACTICES

- Continually analyze devices to uncover system vulnerabilities and criminal behaviors.
- Automatically mitigate risk until the threat is eliminated.

[2] As of early 2016, most devices were still using the older Android versions code-named Jelly Bean (24.7%), KitKat (36.1%), and Lollipop (32.6%). A mere 7% were using the newest version code-named Marshmallow, which was patched to fix 23 vulnerabilities, two of them critical. For details, see OpenSignal, "Android Fragmentation Visualized," August 2015, and Google Developer Dashboard, http://developer.android.com/about/dashboards/index.html, January 2015.

[3] As of early 2016, at least 85% of users had updated to iOS 8, leaving just 15% lagging behind. See OpenSignal, "Android Fragmentation Visualized", August 2015.

[4] Check Point mobile threat intelligence report, 2015. https://www.checkpoint.com/resources/2015securityreport/

2 ROOT ACCESS AND CONFIGURATION CHANGES

Gaining root access to a smartphone or tablet (also called "rooting" with Android or "jailbreaking" with iOS) is no longer only for gadget enthusiasts. Root access enables a wide range of customizations and configurations. It also gives criminals greater access, which exposes devices and data to risk.

Configuration changes, which users might accept when installing legitimate apps or businesses might make to meet policy requirements, can also be used by criminals to stage attacks. Certain configuration settings, such as allowing an Android device to install third-party apps from unknown sources, expose significant vulnerabilities.

Mobile device management (MDM) and enterprise mobility management (EMM) systems, which are used to manage devices, configuration settings, and security policies, offer static root indicators. They work by detecting the existence of certain files in a system directory that enable root access. However, free tools are available for avoiding this type of detection. With root access, cyber criminals can even deny root check requests from the EMM or MDM system, bypassing detection entirely[5].

Enterprises need to look beyond static indicators and use advanced techniques for detecting if and how root access was granted. A comprehensive solution would also monitor all configuration changes and use behavioral analysis to detect unexpected system behavior. This solution should be integrated with your organization's MDM or EMM system to restrict access and make real- time, risk-based policy adjustments on compromised devices that MDM and EMM systems on their own can't detect. A solution that provides dynamic threat response can prevent compromised devices from accessing your company's network.

BEST PRACTICES

- Use both static and dynamic detection methods to determine if root access has occurred and how it occurred.
- Monitor all configuration changes.
- Use behavioral analysis to detect unexpected system behavior.
- Integrate advanced detection with EMM or MDM systems for real-time policy adjustments on compromised devices.

3 REPACKAGED AND FAKE APPS

Malicious apps can take control of mobile devices. The app may not appear to be malicious, and users may not notice or understand the permissions they grant during installation. Even popular apps can be reverse-engineered and injected with malicious code, and then uploaded to an app store under a different name.[6] Repackaged or renamed apps may provide the app's essential functions but also infect the user's device.

[5] For example, Xposed Framework for Android and xCon for iOS.

[6] Flappy Bird, a massively popular Android game, was reverse-engineered to include malware, renamed to a similar name, and uploaded to Google Play. Once discovered, the app was promptly removed by Google, but not before it had been downloaded by unknown numbers of unsuspecting Android users.

Criminals also create seemingly authentic copies of apps that include similar icons, descriptions, screenshots, and even user reviews, but don't work as intended victims get a malicious payload, such as a subscription to an expensive texting service or a stealthy surveillance tool. Malicious apps can enable a host of activities, such as remotely seizing control of the device's camera and microphone to spy on users and their surroundings. Some trustworthy apps can exhibit risky behavior, causing false-positive headaches for security teams and a poor experience for users who might be blocked from using completely safe apps.[7]

Mobile anti-virus protection solutions can uncover malicious code in apps by looking for unique binary signatures, but criminals may have found a way to obfuscate those signatures. Besides, signatures are not yet available for "zero-day" (newlycreated) malware.Yoursolutionmustemployadditionaldetectionmethods,suchasmonitoringtheapp's installation process and determining whether the app actually came from an app store or was installed from some other source.

To ensure productivity with safe apps and still block unsafe apps, you can deploy a solution that captures apps as they are downloaded, and runs each app in a virtual "sandbox" environment to analyze its behavior. A cloud solution can aggregate intelligence about the developer's reputation, the number of downloads, the app source, and the reputation of the servers the app talks to, and then white-list the trustworthy apps automatically so that users can download them without security issues.

BEST PRACTICES

- Uncover malicious code in apps by looking for the unique binary signatures for known malware.
- Determine whether an app came from an app store or some other source, and monitor the app installation process.
- Capture apps as they are downloaded and run them in a "sandbox" environment to analyze their behaviors before flagging them as malicious.
- Aggregate and correlate intelligence about the developer's reputation, the number of downloads, the app source, and the reputation of the app's servers, in order to white-list legitimate apps.

4 TROJANS AND MALWARE

Criminals invest heavily in developing new techniques to install and hide malware. Trojans, carried within an app or installed through an unsecured network connection, infect a device with malicious code that may conduct surveillance by eavesdropping and recording conversations, extracting call logs, tracking locations, logging keyboard activity, and collecting passwords.

An app's code is like a tremendous map of virtually infinite routes. The logic of one line of code may have dozens or even thousands of touch points, all within the same app. This makes it difficult to understand if any of these routes are designed to install a trojan or trigger malicious activity. To expose malicious code, you can deploy a solution that captures apps and reverse- engineers them automatically. This creates a blueprint for

[7] Facebook, for example, syncs and uploads contacts and calendar details, and even records voice during status updates. Although this behavior is associated with the most aggressive types of malware, Facebook isn't malicious.

semantic analysis that can identify suspicious patterns and behaviors. For example, advanced code-flow analysis can expose whether hard-coded phone numbers are used to contact premium messaging services, or if the code is using the device microphone to record sound files it then sends to nefarious external servers.

To mitigate risks already found in devices, you can automate responses and user notifications on the devices with remediation steps, or dynamically trigger device policy changes in your MDM or EMM solution. You should also block traffic to malicious servers to contain the attack so that users can continue using their devices until remediation is complete.

BEST PRACTICES

- Capture and reverse-engineer apps for code-flow analysis to expose any suspicious behavior.
- Automate responses and user notifications with remediation steps to remove the malware.
- Dynamically trigger device policy changes in your MDM or EMM solution.
- Block traffic to malicious servers to contain the attack.

5 MAN-IN-THE-MIDDLE ATTACKS

Man-in-the-middle attacks can eavesdrop, intercept and alter traffic between two devices. You believe you are interacting with a known and trusted entity, but an attack is copying credentials, snooping on instant messages, or stealing sensitive information. The familiar alert and warning signs on PCs and laptops are far more subtle and easily overlooked on mobile devices. Small screen sizes can hide web addresses, making it harder to validate the address the browser is pointing to.

Public Wi-Fi hotspots, which are convenient for internet access, are easy to fake. An attacker can create a spoofed Wi-Fi network, or eavesdrop and alter a legitimate network's encrypted communications by using spoofed certificates or downgrading the communication link so that it is no longer encrypted.[8] The attacker can then intercept communications, alter data in transit, or install a trojan.

You need behavioral analysis that can detect rogue hotspots and malicious network behavior and conditions, and automatically disable suspicious networks to keep devices and your data safe. Your solution should validate the integrity of secure connections to detect compromises, and use a cloud-based honeypot—a system set up to attract and identify attackers who try to penetrate your network. You may also want to dynamically trigger a secure virtual private network (VPN) on the device to protect the privacy and integrity of communications and minimize the impact of an attack.

[8] SSL (Secure Sockets Layer) is a standard for establishing an encrypted link between a server and a client typically a website and a browser, or a mail server and a mail client (such as Outlook). SSL stripping circumvents automatic redirection to secure connections, and SSL bumping uses fake certificates to fool apps and browsers into believing they're using private web connections. Both of these attacks can leave sensitive data unprotected.

BEST PRACTICES

- Use behavioral analysis to detect rogue hotspots and malicious network behavior.
- Automatically disable suspicious networks to keep devices and your data safe.
- Validate the integrity of secure connections to detect compromises.
- Use a cloud-based honeypot to attract and identify attackers.
- Use on-device remediation to dynamically trigger a secure VPN that protects the privacy and integrity of your communications.

CONCLUSION

Many companies enforce basic mobile hygiene policies using mobile device management to address security and bring-your-own-device issues. Some augment this management with a hodgepodge of point solutions that offer incremental and often rudimentary enhancements. These solutions may control the potential damage inflicted by lost or stolen devices, but they address risks only on the surface.

Comprehensive mobile security should be a system of components that work together cohesively to identify a wide variety of threats and to protect data while addressing employee privacy concerns. Only solutions that can analyze behavior across all vectors for indicators of attack can protect mobile devices effectively to keep them safe.

Check Point SandBlast Mobile is a multilayered security infrastructure that provides comprehensive protection. It identifies threats using on-device, network- and cloud-based algorithms, and triggers automatic defense responses. Its cloud based risk engine identifies suspicious patterns and behaviors over time by sandboxing apps in an emulator and detecting threats at the device, app, and network levels. The infrastructure integrates with existing secur- ity investments to support incident response and provide continuous protection. As a result, organizations always have an accurate picture of the types of threats devices on their network are facing, as well as detailed information about what is being done to mitigate those risks.

More Information: www.caldoo.nl/sandblast-mobile/