CHECK POINT
THE TOP 4 CYBER SECURITY THREATS TO ANDROID MOBILE DEVICES

Understand the Impact of Exploits and How to Protect Your Organization

A recent study by Check Point Mobile Security and a global cellular network provider[1] found that **one in 1000 devices were infected** with mobile surveillance and mobile Remote Access Trojans (mRATs). These attacks were found on both Android and iOS devices; the prevalence of Android-based devices **(over 80% of the worldwide phone market; 60% of the tablet market)**[2]makes it important to understand the risks they can pose to an organization. The following is a high-level overview of the four most common types of attacks that impact Android mobile devices and the basic requirements for protecting against them:

1. MOBILE REMOTE ACCESS TROJANS (MRATS)

These attacks, as their name implies, can give an attacker the ability to remotely gain access to everything stored on and flowing through the device.

These attacks are typically downloaded from application markets, including Google marketplaces, such as Google Play. Legitimate and seemingly innocuous apps can contain the malicious functionality. Once downloaded, the malicious code can be activated by the attacker and used to do almost anything on the device.

A device of an executive or critical employee infected with an mRAT can have a severe impact on the business – the attacker could be privy to all sorts of sensitive information. They could turn on the device's recording functionality to listen in on boardroom discussions, forward emails or text messages sent to or by the device, take photos of whiteboard diagrams from meetings, access phone calls and voice mails, and even track that individual's whereabouts.

While Google has been working hard to protect the Google Marketplaces from mRATs, with regular security code checks, there are simply too many apps to monitor. (There are more than 1.2 billion Android apps in the Google Play market, with approximately 30,000 being added monthly.[3]) Plus, there are no built-in security code checks for those apps downloaded through secondary markets.

1. The study sampled 650K randomly selected subscribers in the EMEA region.
2. IDC and Gartner market share numbers.
3. AppBrain Statistics - http://www.appbrain.com/stats/number-of-android-apps

As a result, it is important to have a solution that can analyze the behavior of applications on the device, as well as correlate events on the device and in the network to identify suspicious activity – such as traffic going to unknown servers.

2. SYSTEM EXPLOITS - ELEVATED PRIVILEGES

System vulnerabilities can be exploited by an attacker to gain elevated privileges (equivalent to 'rooting' the device) without leaving a trace. In the past year, a dozen such exploits were released, including a tool that exploited a vulnerability on devices running Android 4.0-4.4, a vulnerability in the pre-installed backup software on LG devices, and a vulnerability in the drivers used by the camera and multimedia devices on Exynos 4-powered devices. (Learn about the 2013 Android vulnerability of the year.)

The attacks take advantage of opportunities created by the fragmentation of the Android operating system and the openness and vastness of its eco-system. All the different devices and vendor implementations of Android have fragmented the operating system and broken the security patch delivery model. The irregularity of hardware patching cycles and the variances from platform to platform offer attackers ample infection vectors to exploit.

In addition, while Google has been working hard to protect its Marketplace from attacks, such as mRATs, by performing security code checks, Google does not perform any built-in security code checks for the apps downloaded from the dozens of secondary open app markets.

Protecting Android devices requires a solution that can cover all the different potential threat vectors. It needs to be able to detect malicious applications and vulnerability exploits that could impact a specific device (given the device type, OS version, patch levels, and implementation). It should also be able to correlate device, network and event information to detect and prevent system-level attacks.

3. WIFI MAN IN THE MIDDLE (MITM)

A MitM attack occurs when the device connects to a rogue WiFi hotspot. Since all communications are passed through the attacker-controlled network device, they can eavesdrop and even alter the network's communication.

MitM attacks have always been a concern for wireless devices, however, the prevalence of smartphones in an individual's personal and business life has made mobile devices much more attractive targets for this attack.

Unfortunately, the typical alert and warning signs that individuals are used to seeing on PCs and laptops are much more subtle in their mobile counterparts. For example, the limited screen real-estate of mobile devices often hides URLs from the user, so they don't validate the URL the browser is pointing to is actually the intended one.

The best way to thwart these types of attacks is through the use of a VPN to encrypt and isolate the communications. Ideally the VPN would be triggered only when rogue hotspots and other risk factors are detected to maximize the user experience.

CONTACT US
Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

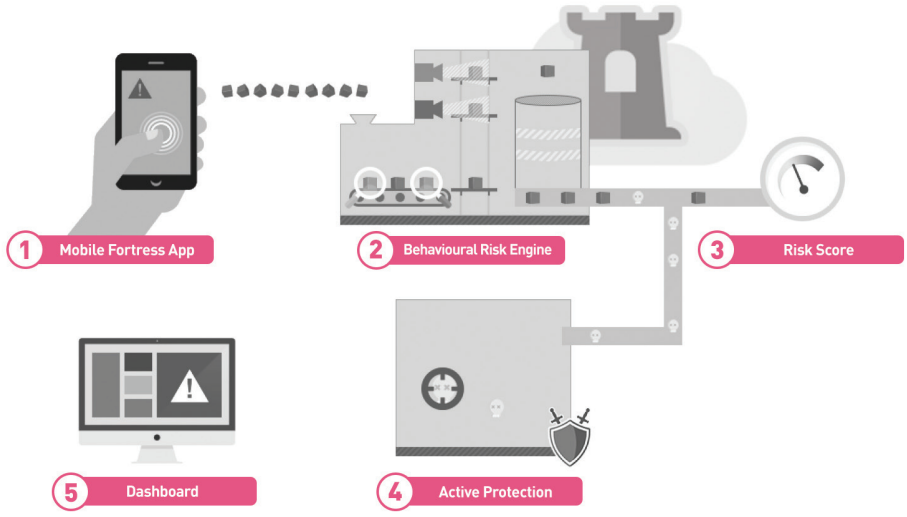
4. ZERO-DAY ATTACKS

Zero-day attacks represent exploits of vulnerabilities that have been uncovered – but not yet released. Many times, these vulnerabilities lead to the silent installation of attacks, such as mRATs, on a device through a remote exploitation technique.

Once on the device, they may enable the attacker to steal passwords, corporate data and emails, as well as capture all keyboard activity (key logging) and screen information (screen scraping). They may also activate the microphone to listen in on conversations and meetings, or act as a botnet to steal contacts or text messages (SMS texts).

AV solutions, which rely on known attack patterns to detect attacks, are unable to provide protection for unknown attacks. Organizations need a solution that can identify any suspicious behavior from an app, a device or the network to find and mitigate the impact of zero-day mobile exploits.

ABOUT CHECK POINT MOBILE SECURITY – COMPREHENSIVE PROTECTION AGAINST MOBILE THREATS TO ANDROID



Check Point Mobile Security provides a mobile threat management platform that allows enterprises to easily manage and mitigate the risks of BYOD and protect their corporate assets from mobile cyber threats, such as malicious applications, targeted network attacks and advanced persistent threats (APTs). Check Point not only provides the most comprehensive solution for iOS and Android, but also delivers real-time mobile security and intelligence to an organization's existing security and mobility infrastructures. Its patented technology detects device, application and in-network threats that others will miss and quantifies the risks and vulnerabilities that BYOD exposes to the enterprise. With Check Point, enterprises can balance the needs of mobile security and protection, without impacting the end user's experience and privacy, to confidently embrace BYOD and other mobility initiatives to fuel their business.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com