Attacks on your mobile devices and traffic are quickly evolving. Mobile attackers are stealing (hey, it’s what they do) tried and true methods from the “traditional” (wired) world and applying them to the mobile one, as well as coming up with new, never before seen tactics that really take advantage of the new pathways mobile devices offer into an organization’s network. You need to prevent all the ways an attacker can exploit mobile devices to:

- **Eavesdrop**
  - Take over your device’s microphone and camera

- **Collect Enterprise Data**
  - Including emails, texts and call logs

- **Compromise Secure Containers**
  - Extract application data

The following is a quick look at some of the most common types of mobile attacks and what you need to arm yourself with to prevent them.

### Android Malware Applications

<table>
<thead>
<tr>
<th>WHAT IT DOES AND HOW IT WORKS</th>
<th>INFECTION VECTORS – HOW IT ‘GETS IN’</th>
<th>DAMAGE IT CAN CAUSE</th>
<th>HOW TO DETECT AND PREVENT IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>These are malicious applications installed on a device using the Android operating system (OS). The malware usually disguises itself as an innocent app, such as a game, conference or PDF viewer, and then runs in the background doing all its malicious activity.</td>
<td>The malicious applications may be downloaded from Google Play or a 3rd party app store, an e-mail, or an infected website or ad network. The malicious applications may also be uploaded by an attacker who gains physical access to the device. (Sometimes your kids/nephews/nieces/etc. install it!)</td>
<td>Malware applications can act as a remote access Trojan, with a surveillance toolkit that can enable the attacker to steal passwords, corporate data and emails, as well as capture all keyboard activity (keylogging) and screen information (screen scraping). They may also activate the microphone to listen in on conversations and meetings, act as a Trojan to steal contacts or text messages (SMS texts), or act as a mobile botnet to send SMS messages to premium numbers.</td>
<td><strong>DETECT:</strong> You need a combination of AV, Network and Event Anomaly Detection, and Behavioral Application Analysis (Sandboxing and advanced code and traffic analysis) to be able to detect the wide variety of malicious applications potentially in your environment. <strong>PREVENT:</strong> You need On-Device Remediation that can enable users to remove malware already on their device, as well as Network-Based Mitigation to block any exfiltration activity.</td>
</tr>
</tbody>
</table>
## ANDROID ROOTKITS (NON-APPLICATION MALWARE)

<table>
<thead>
<tr>
<th>WHAT IT DOES AND HOW IT WORKS</th>
<th>INFECTION VECTORS – HOW IT ‘GETS IN’</th>
<th>DAMAGE IT CAN CAUSE</th>
<th>HOW TO DETECT AND PREVENT IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Rootkits are malicious software designed to enable privileged (root) access to a device using vulnerabilities in the Android OS, without being detected. Once deployed on the device they look like an Android OS system file (they usually load themselves into the system directory) and cannot be removed without actually doing a factory reset to the device. This makes them invisible to AV-based solutions because privileged access is required to scan the locations where the rootkit is installed.</td>
<td>Rootkits may be embedded in apps downloaded from Google Play or a 3rd party app store, an e-mail, an infected website or ad network. The Rootkits may also be pre-installed on the device or uploaded by an attacker who gains physical access to the device. Once on the device, the Rootkits use an exploit to break the operating system application sandbox and install themselves deep in the OS.</td>
<td>Rootkits can act as a remote access Trojan, with a surveillance toolkit that can enable the attacker to steal passwords, corporate data and emails, as well as capture all keyboard activity (keylogging) 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).</td>
<td>DETECT: You need the ability to do Network and Event Anomaly Detection, as well as Behavioral Application Analysis to detect abnormal activity on a device, including communications from binaries that are not applications, and correlate that activity with events on the device to detect malware that resides at the system-level. PREVENT: You need to be able to block the communication of non-application malware to contain the threat.</td>
</tr>
</tbody>
</table>

---

## EXPLOITS

<table>
<thead>
<tr>
<th>WHAT IT DOES AND HOW IT WORKS</th>
<th>INFECTION VECTORS – HOW IT ‘GETS IN’</th>
<th>DAMAGE IT CAN CAUSE</th>
<th>HOW TO DETECT AND PREVENT IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>These span a large number of attacks that utilize vulnerabilities in the operating system (OS) to enable attackers to gain elevated privileges (root) and break the OS’ application Sandbox.</td>
<td>Exploits may be disguised in applications downloaded from Google Play or a 3rd party app store, an e-mail, or an infected website or ad network. The Exploits may also be uploaded by an attacker who gains physical access to the device.</td>
<td>Once the exploit executes, the attacker can snoop into other applications storage, memory and resources, thus gaining access to encrypted enterprise content within Mobile Device Management (MDM) solutions, Containers and Wrappers. Basically they have access to everything stored on or flowing through the mobile device.</td>
<td>DETECT: You need Behavioral Application Analysis and Sandbox analysis of payloads. The Sandbox needs to be able to uniquely behave like the attacked device to mitigate VM detection. PREVENT: You need On-Device Remediation to enable users to remove malware already on a device and block any exfiltration activity. Can use Network-based Mitigation to block exploit traffic to contain attack.</td>
</tr>
</tbody>
</table>
iOS malware delivered using fake certificates is malicious software installed on a device using the Apple iOS operating system (OS) that is accompanied by certificates validated by Apple that actually represent a trusted organization that has been compromised. Ever heard of Sutxnet, Flame and Bit9 attacks? – they used a method similar to this.

Apple grants two different 3rd party certificates to organizations that agree to adhere to Apple’s guidelines. They are:

1. Developer certificates, which allow developers to test their apps before they go public on the Apple app store.
2. Enterprise certificates, which provide organizations the opportunity to establish their own, in-house marketplace for dedicated apps.

Behind the scenes, Apple validates an app is signed by a trusted certificate before allowing it to be side-loaded (which means it’s not installed through the App Store) on the device.

If an attacker is able to obtain a certificate they can use it to validate their malware and install it on any iOS device without passing it through the vetting process in the App Store. A user can then be lured to download their seemingly harmless app. (Note, given the volume of apps, it is very difficult for Apple to monitor the use of certificates, as a result, attacks have started to emerge, such as FinFisher mRAT that use these certificates.)

This malware can be used to do almost anything. It can act as a remote access Trojan, with a surveillance toolkit that may enable the attacker to steal passwords, emails, calendar records and geo-location, in real time. It can even activate the microphone to listen in on conversations and meetings.

**DETECT:** You need Device Risk Assessments that can detect iOS apps on the device that are using stolen or fraudulent Enterprise/Developer certificates.

**PREVENT:** You need On-Device Remediation that can block or remove fraudulent certificates to eliminate the attack.
## iOS Malicious Profiles

<table>
<thead>
<tr>
<th>WHAT IT DOES AND HOW IT WORKS</th>
<th>INFECTION VECTORS – HOW IT ‘GETS IN’</th>
<th>DAMAGE IT CAN CAUSE</th>
<th>HOW TO DETECT AND PREVENT IT</th>
</tr>
</thead>
</table>
| An attack that uses a configuration file for iOS that can re-define system functionality parameters, such as device, mobile carrier, mobile device management (MDM) and network settings. A profile can circumvent device and or application security mechanisms, which is why it’s an attractive target for attackers. | A user may be tricked into downloading a malicious profile and, by doing so, unknowingly provide the rogue configuration the ability to re-route all traffic from the mobile device to an attacker-controlled server, further install rogue apps or even decrypt communications. A profile can also be loaded by an attacker, who gains physical access to the device. | A malicious profile circumvents typical security mechanisms, so it can be used to do almost anything. It can enable the attacker to steal passwords, emails, all data stored or passed through the phone, calendar records and geo-location, in real-time. | DETECT: You need Device Risk Assessments that can detect rogue iOS profiles or profiles that have been altered on the device. Behavioral Application Analysis can also be used to identify profiles that exhibit abnormal or suspicious activity.  
PREVENT: You need On-Device Remediation that can block or remove malicious profiles to eliminate the attack. |

## iOS Surveillance and Mobile Remote Access Trojans (MRATs)

<table>
<thead>
<tr>
<th>WHAT IT DOES AND HOW IT WORKS</th>
<th>INFECTION VECTORS – HOW IT ‘GETS IN’</th>
<th>DAMAGE IT CAN CAUSE</th>
<th>HOW TO DETECT AND PREVENT IT</th>
</tr>
</thead>
</table>
| iOS mRATs are malicious software installed on a device using the Apple iOS operating system (OS) that gives an attacker the ability to remotely gain access to everything stored and flowing through the device. | These attacks typically take advantage of a device that has been jailbroken, which means all the built-in iOS security mechanisms have been removed. It’s not unusual for iOS users to jailbreak their own device, so they can install any iOS application they want, not just the ones that are from Apple’s proprietary store. Attackers can also jailbreak an iOS device themselves, by physically obtaining access to the device or propagating the jailbreak code from a compromised computer through a USB cable. Once jailbroken, attackers can install the surveillance or spyphone application of their choice, or disguise it in an application from a third party app store for an unwitting user to download. | mRATs can act as a remote access Trojan, with a surveillance toolkit that can enable the attacker to steal passwords, corporate data and emails, as well as capture all keyboard activity (keylogging) 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). | DETECT: You need to conduct Device Risk Assessments to detect those devices that have been jailbroken and then investigate the actual behavior of the communication on the device.  
PREVENT: You need both On-Device Remediation and Network-based Mitigation to actively block traffic and contain the mRAT. |
# Man-in-the-Middle (MitM)

<table>
<thead>
<tr>
<th>WHAT IT DOES AND HOW IT WORKS</th>
<th>INFECTION VECTORS – HOW IT 'GETS IN'</th>
<th>DAMAGE IT CAN CAUSE</th>
<th>HOW TO DETECT AND PREVENT IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MitM attacks can eavesdrop, intercept and alter traffic between two computing devices. The user believes they are interacting with a known, trusted entity (typically a web site). The normal alert and warning signs on PCs and laptops are much more subtle on mobile devices and their limited screen size often hides URLs from the user, making it harder to validate the URL the browser is pointing to is actually the intended one.</td>
<td>WiFi MitM attacks occur when a mobile device connects to a rogue WiFi hotspot. The attacker may create a spoofed WiFi network (e.g. 'Free-Starbucks') or simply connect to the same legitimate WiFi the victim is using; regardless all communications end up passing through the attacker-controlled network device.</td>
<td>MitM attacks can be used to eavesdrop and even alter the encrypted (SSL) network’s communication by using spoofed certificates or downgrading the communication link, so it’s un-encrypted and completely open to the attacker.</td>
<td>DETECT: You need Behavioral Application Analysis that can detect rogue WiFi hotspots and other risk factors. PREVENT: You need On-Device Remediation that can dynamically trigger a VPN to isolate the user’s communication from the compromised network and Network-based Mitigation to block traffic from a rogue hotspot.</td>
</tr>
</tbody>
</table>

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

©2015 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]