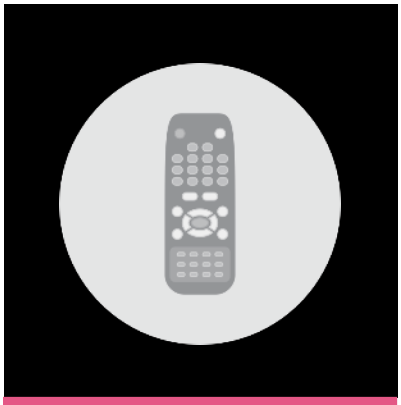
THE TOP 6 CYBER SECURITY THREATS TO IOS DEVICES



ONE IN 1000 DEVICES IS INFECTED WITH MOBILE SURVEILLANCE AND MOBILE REMOTE ACCESS TROJANS (MRATS).

A recent study[1] found that one in 1000 devices is infected with mobile surveillance and mobile Remote Access Trojans (mRATs). These attacks are found on both Android and iOS devices; in fact 47% of the infected devices were iOS-based, challenging the assumption that an operating system's security measures make it impervious to exploits. The following is a summary of the six most common types of attacks that impact iOS mobile devices and the basic requirements for protecting against them:

1. iOS Surveillance and Mobile Remote Access Trojans (mRATs)

These attacks jailbreak a device, which removes all the built-in iOS security mechanisms, and install surveillance and mRAT software that gives the att acker the ability remotely to gain access to everything stored and flowing through the device.

Attackers can jailbreak the device by physically obtaining access or by propagating the jailbreak code from a compromised computer through a USB cable. However, It may be the attacker does not need to jailbreak the device themselves - device owners are quite notorious for their desire to jailbreak their mobile phones and tablets. For example, in February 2013, a jailbreaking technique, nicknamed Evasi0n, garnered 7M hacked devices in just four days.

Once jailbroken, any iOS-app from any app marketplace can be installed on the device –not just those apps approved by Apple in their proprietary app store. A popular alternative app market is Cydia, but many others exist. These markets offer a variety of legitimate apps, however, they also contain hundreds of seemingly innocuous apps that hide malicious functionality. Users downloading these apps are unknowingly infecting their own devices with mRATs.

No mobile AV exists to protect against these threats. The problem is exacerbated by the fact a jailbreak can easily be hidden from Mobile Device Management (MDM) solutions. For example, popular forums, such as xCon, freely provide methods to circumvent MDM detection. What's needed is a way to detect accurately when a device has been jailbroken and the ability to identify surveillance behavior.

[1] The study sampled 650K randomly selected mobile subscribers in the EMEA region.

IT IS SIMPLY **NOT POSSIBLE** FOR APPLE TO MONITOR THE INSTALLATION OF EVERY DEVELOPER AND ENTERPRISE APPLICATION AND CERTIFICATE.

2. Fake iOS Enterprise or Developer Certificates

These attacks use distribution certificates to 'side-load' an application (with malware), which means it does not have to go through Apple's app store validation process and can be downloaded straight onto the device.

Apple provides two different 3rd-party certificate types - developer and enterprise – to try to maintain the integrity of the apps in their store. Developer certificates allow developers to test their apps before they go public in the app store while enterprise certificates provide organizations the opportunity to establish their in-house marketplace for dedicated apps.

Behind the scenes, iOS validates that a trusted certificate signs each app before allowing it. Problems occur when an attacker can obtain (e.g. by stealing or buying on the black market) a certificate for their malware. They can then lure the user to download their seemingly harmless app and unknowingly infect their device; because the certificate accompanies the app, it is validated and easily installed, without barriers.

This method has already been seen in use. In mid-2013, a rogue Chinese site used an enterprise certificate to distribute pirated iOS-based apps. It has also been revealed the FinFisher mRAT used developer cert in its exploitation.

It is simply not possible for Apple to monitor the installation of every developer and enterprise application and certificate, so it comes down to having a solution that can detect, block and remove apps using stolen or fraudulent certificates.

3. Malicious iOS Profiles

These attacks leverage the permissions of a profile to circumvent typical security mechanisms to do almost anything ultimately. A profile is an extremely sensitive optional configuration file that can re-define different system functionality parameters, such as mobile carrier, MDM and network settings.

A user may be tricked into downloading a malicious profile. In doing so, he may unknowingly provide the rogue configuration the ability to re-route all traffic from the mobile device to an attacker-controlled server, to further install rogue apps, and even to decrypt communications.

Any changes to a profile need to be flagged and carefully considered, even when seemingly innocuous. At one time, LinkedIn introduced an iOS app that made changes to the device's profile to reroute all email through their servers. Linkedin discontinued it three months after its introduction, due to the controversy over it's capabilities. To prevent data exfiltration, a solution needs to be in place that can not only detect rogue or altered profiles, but also block and remove them to eliminate the threat.

ANTIVIRUS SOLUTIONS, WHICH RELY ON KNOWN ATTACK PATTERNS, ARE UNABLE TO PROVIDE PROTECTION FOR UNKNOWN ATTACKS.

4. 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 do not 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.

5. WebKit Vulnerabilities

WebKits enable web browsers to render web pages correctly for a user. Attackers will exploit vulnerabilities in a Webkit to execute scripts of their own. Attackers commonly use them as a springboard for remote device infection.

An example of a WebKit was the popular iOS4 jailbreaking technique, named JailbreakMe. It took advantage of flaws in the Safari browser to enable users to jailbreak their device when they visited a dedicated website. To prevent malicious WebKit exploits requires a solution that can identify suspicious behavior and correlate activity with events on the device and network and then stop any data being sent to the attacker.

6. Zero-Day Attacks

Zero-day attacks represent exploits of vulnerabilities that have been uncovered – but not yet released. With vulnerability researchers earning purportedly $500K per vulnerability, the race towards exposure is in full throttle.

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.