

Threats to iOS Mobile Devices

A recent study by Lagoon Mobile Security and a global cellular network provider 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; 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 some of the most common types of attacks that impact iOS mobile devices:



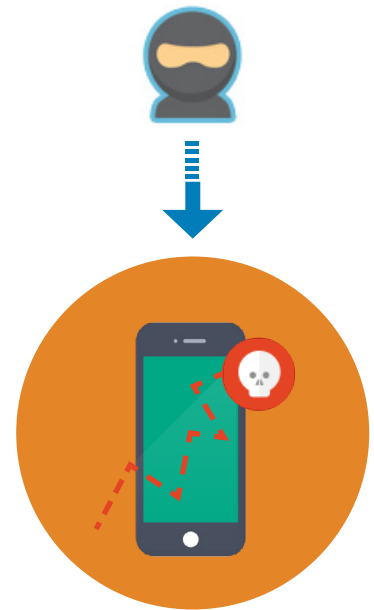
iOS Surveillance and Mobile Remote Access Trojans (mRATs)

These attacks jailbreak a device, which removes all the built-in iOS security mechanisms, and install surveillance and mRAT software that gives the attacker the ability to remotely 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 doesn't need to jailbreak the device themselves - device owners are quite notorious for their [desire](#) to jailbreak their own mobile phones and tablets. For example, in February 2013, a jailbreaking technique, nicknamed [EvasiOn](#), 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 accurately detect when a device has been jailbroken and the ability to identify surveillance behavior.



Secure Your Organization
from All Mobile Threats

Lagoon Security Inc.
350 Rhode Island Street
South Tower, Suite 240
San Francisco, CA 94103
Sales and Support
US: +1-855-888-5882
UK: +44-800-680-0630
sales@lagoon.com

Threats to iOS Mobile Devices (cont.)

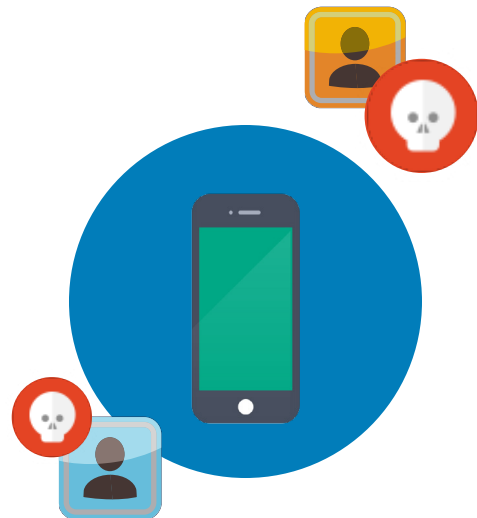
Fake iOS Enterprise or Developer Certificates

These attacks use distribution certificates to 'side-load' an application (with malware), which means it doesn't 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 own in-house marketplace for dedicated apps. Behind the scenes, iOS validates that each app is signed by a trusted certificate before allowing it.

Problems occur when an attacker is able to 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 app is accompanied by the certificate, it is validated and easily installed, without any iOS 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](#) a developer certificate 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 and block/remove iOS apps that are using stolen or fraudulent certificates.



Malicious iOS Profiles

These attacks leverage the permissions of a profile to circumvent typical security mechanisms to ultimately do almost anything. 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 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, and even decrypt communications.

Any changes to a profile need to be flagged and carefully considered, even when seemingly innocuous - recently, LinkedIn introduced an iOS app that made changes to the device's profile to reroute all email through their servers ([Check out the Lacon FAQ on LinkedIn Intro.](#)) 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.

Threats to iOS Mobile Devices (cont.)

WiFi Man in the Middle (MitM) - iOS Threat

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.

WebKit Vulnerabilities - iOS Threat

WebKits enable web browsers to correctly render web pages for a user. Attackers will exploit vulnerabilities in a Webkit to execute scripts of their own. They are commonly used by attackers as a springboard for the remote infection of the device.

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.



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.

Zero-Day System Vulnerabilities - iOS Threat

Zero-day vulnerabilities are those vulnerabilities that have been uncovered - but not yet released. With vulnerability researchers [earning](#) purportedly \$500K per vulnerability, the race towards vulnerability 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.

About Lagoon Mobile Security – Comprehensive Protection Against Mobile Threats to iOS



Lagoon Mobile Security is pioneering a new class of security solutions that comprehensively protects mobile devices, both iOS and Android, from known, zero-day, advanced targeted threats. Lagoon uses several proprietary, patent-pending algorithms to conduct multi-level risk assessments to detect the wide range of mobile infection vectors and then

provides active protection capabilities on the device and in the network to mitigate any threat. With Lagoon, organizations can prevent cyber espionage and data exfiltration from their mobile devices and confidently embrace BYOD and other mobility initiatives to fuel their business.

