Malicious Profiles - The Sleeping Giant of iOS Security »

By Posted by Yair Amit

Published: 2013-03-12 · Archived: 2026-04-05 23:34:03 UTC

Malware is prevalent. Mobile malware is on the rise. We are used to the perception that Android users are always under the threat of being attacked by malware and therefore should be highly suspicious about the software they install, while iOS users are immune and can enjoy the freedom of installing whatever they want without hesitation, due to Apple's "walled-garden" approach. Well… this isn't exactly the case.

As I'll further discuss in this post, there is another way to create havoc on one's device, which may be comparable to sophisticated malware, without actually installing a program on the device.

Background

When discussing mobile malware, which keeps getting more attention as time goes, we usually think about Android. While the iOS app-store has been hit by viruses in the past, this phenomena is certainly negligible nowadays (though we believe this can change as well, more on that in future blog posts).

Thanks to Apple's application review process and app sandboxing, iOS users are in a pretty good condition when it comes to security. The application review process makes it harder for attackers to insert malicious apps to Apple's App Store. Moreover, app sandboxing makes sure that malicious applications have limited permissions and capabilities if and when they reach to an iOS device. As demonstrated in the diagram below, a sandboxed application has access to restricted resources and cannot change system-level settings.

Source: Apple's app sandbox design guide

iOS profiles, also known as mobileconfig files, are used by cellular carriers, Mobile Device Management solutions and even mobile applications, in order to configure key system-level settings of iOS devices. These include Wi-Fi, VPN, Email and APN settings, among others. While mobileconfigs are usually used for constructive needs and thus provide a lot of value, these same capabilities might be used by malicious attackers to circumvent Apple's security model and perform significant damage to their victims.

Impact

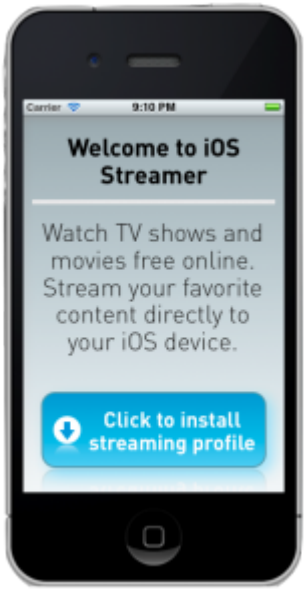
A malicious profile could be used to remote control mobile devices, monitor and manipulate user activity and hijack user sessions. In addition to being able to route all of the victim's traffic through the attacker's server, a more interesting and hazardous characteristic of malicious profiles is the ability to install root certificates on victims' devices. This makes it possible to seamlessly intercept and decrypt SSL/TLS secure connections, on which most applications rely to transfer sensitive data. A few concrete impact examples include: stealing one's Facebook, LinkedIn, mail and even bank identities and acting on his/her behalf in these account, potentially creating havoc.

We actually created an online demo that demonstrates the aforementioned. We believe it can give a good sense of the severity and ease of the attack. If you would like to get more information, feel free to leave us a note at contact@skycure.com and we'll gladly follow-up with you.

Infection Scenarios

Luring victims to install a malicious mobileconfig is rather simple, as attackers can utilize their accumulated knowledge in social engineering. Here are two examples for common techniques:

1. Victims browse to an attacker-controlled website, which promises them free access to popular movies and TV-shows. In order to get the free access, "all they have to do" is to install an iOS profile that will "configure" their devices accordingly.
2. Victims receive a mail that promises them a "better battery performance" or just "something cool to watch" upon installation.



Sample profile-based iOS malware attack

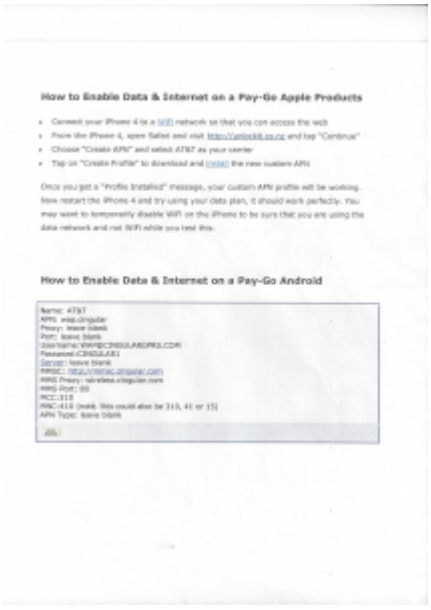
Not surprisingly, the aforementioned is very similar to the way viruses have been circulating in the Internet for many years now.

However, we identified another possible infection vector, which can prove to be very effective due to its reliance on the trust between customers and their service providers. A quick survey we did uncovered a variety of cellular

carriers, many of them MVNOs, that ask their clients to install mobileconfig files in order to receive data plan access; unfortunately, these processes usually involve poor utilization of security measures. As part of our work, we identified a worrisome process at several AT&T stores, which is further described below. As part of our responsible disclosure process, we notified and worked with AT&T to address our findings. We would like to further mitigate the exposure for such threats by raising awareness among both AT&T and non-AT&T clients.

Insecure iOS profile installation process: AT&T as a case-study

We recently witnessed a problematic procedure at several AT&T stores we visited. As pay-as-you-go clients who own an iPhone, we were directed to download and install profiles on our own devices. According to AT&T's instructions (see below a copy of an instructions document we received from an AT&T salesperson in Manhattan), users are advised to download a profile from http://unlockit.co.nz via an unencrypted channel. The installation of this mobile configuration, which configures APN settings on the device, is mandatory for granting access to AT&T's data network. In one of the stores, an AT&T salesperson actually took our phone and performed the aforementioned process via a public wi-fi network, which is an easy target for man-in-the-middle attacks.


How to Enable Data & Internet on a Pay-Go Apple Products

How to Enable Data & Internet on a Pay-Go Android

Source: AT&T store, Manhattan

What is wrong with the aforementioned process?

Due to the capabilities of mobileconfig profiles, a connection to an external resource for the purpose of downloading and installing profiles on iOS-based devices should always be thought of carefully. The specific interaction with http://unlockit.co.nz is done over plain text (without an SSL/TLS encryption layer). As well known, man in the middle attacks could be used to alter the mobileconfig downloaded to the phone, allowing the attacker to install a malicious mobileconfig on the user's device without his/her consent or knowledge. This can be easily done by utilizing attacks such as ARP-poisoning and evil twin against the wi-fi network the customer uses for installing the profile, such as AT&T's in-store wi-fi or an Internet cafe network.

During our discussion with AT&T's security team on that matter, they expressed that AT&T's formal policy does not allow prepaid iOS devices offerings. However, given the fact the AT&T stores we visited didn't seem to

follow this policy, we believe AT&T will strive to better enforce it in its stores going forward. We would like to thank AT&T's security team for their cooperation and commitment to the security of AT&T's customers.

Endnote

By taking into consideration the great amount of sensitive actions we perform and the data we store on our mobile devices along with the ease of taking advantage of users' innocence to perform malicious profile attacks, we get to the conclusion that the days of mass exploitation of this attack vector are getting close. Therefore, we find it important to raise awareness to the threats and discuss possible mitigations.

In order to mitigate the risk of malicious profiles, you should strive to follow the next three thumb rules:

1. You should only install profiles from trusted websites or applications.
2. Make sure you download profiles via a secure channel (e.g., use profile links that start with https and not http).
3. Beware of non-verified mobileconfigs. While a verified profile isn't necessarily a safe one, a non-verified should certainly raise your suspicion.

If you identify a suspicious profile, we encourage you to send us the details of the profile and the origin you downloaded it from to security@skycure.com. We will scan it and get back to you with our findings.

Hertzliya Conference

+Adi Sharabani plans to present our findings at the Hertzliya conference cyber security track led by Yuval Ne'eman's Workshop later on today – if you happen to attend the conference, you are most welcome to join us for a quick chat.
