National Computer Board
Computer Emergency Response Team of Mauritius (CERT-MU)
Targeted Security Alert

YiSpecter Malware Targets Apple iOS Devices

Original Issue Date: October 06, 2015

Severity Rating: High

Affected Systems:

- Apple iOS devices

Description:

A new piece of malware known as YiSpecter (IOS.Specter) targeting iOS devices has been discovered. The malware is designed to target Chinese speakers and has affected East Asia, particularly China and Taiwan. The threat is being distributed through different app stores, forum posts, and social media. In addition, hijacked internet service provider (ISP) traffic is also redirecting users to download YiSpecter.

YiSpecter is a Trojan horse for both jailbroken and non-jailbroken iOS devices, which is designed to perform a range of functions. It essentially provides the basis for a back door onto the compromised device and installs adware. The Trojan can allow an attacker to perform a range of functions such as uninstalling existing apps, downloading and installing new fraudulent apps, displaying advertising in other apps that are installed on the device, and much more.

Features of the malware:

1. ***Targets non-jailbroken devices through enterprise certificates***

YiSpecter is an iOS threat that takes advantage of the enterprise app provisioning framework. In legitimate uses of the framework, businesses can benefit from enterprise certificates to provide private apps to their own workforce without making them publicly available on the official App Store. Apps built and signed with the certificates do not need to be vetted by Apple before being distributed outside of the App Store. This gives the certificate owner more scope to develop apps with features that would otherwise be rejected by Apple.

Once YiSpecter's creators have the enterprise certificate, they are able to create and distribute their apps to potentially any iOS device without further oversight from Apple. It should be noted that if Apple learns of the misuse of an enterprise certificate, the company could instantly revoke the certificate and render the signed apps useless.

A common feature of enterprise-signed apps is that they can generally only be installed after the user accepts the request to trust the app or developer.

2. The malware invokes Private APIs

The malware can carry out a lot of advanced functionality because it uses Apple's own private APIs to perform activities that standard iOS apps cannot. These APIs are designed to allow Apple's apps to carry out a range of system-level actions. Any third-party apps that use these private APIs are rejected from inclusion on the Apple App Store. YiSpecter ignores the official App Store, instead relying on unofficial distribution channels to spread the malware. As a result, the threat can take advantage of the private APIs for its own purposes.

3. Potential copycats

By combining two techniques (abuse of enterprise provisioning and invoking private APIs), the potential misuse of the malware is high. Security experts therefore expect to see copycat threats in the future.

Workarounds:

1. iOS device owners are advised not to download and install apps from untrusted sources. Instead, they should only download apps from the official App Store or from their company's own approved app library.

2. Users should avoid jailbreaking their devices. This practice violates the terms of the iOS license agreement and puts the device at an increased risk of attack.

3. Users should also ensure that the device's operating system and software are up to date with latest patches.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info: contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu