Spyware app abused iOS enterprise certificate to track targets

Another app has abused the iOS enterprise certificate in order to bypass Apple's App Store rules, security researchers at Lookout announced on Monday. The app is called Assistenza SIM and it could steal a user's contacts, videos, photos, and real-time location data, as reported by *TechCrunch*. It could also tap people's phone calls remotely.

After researchers contacted Apple, the company revoked the app's enterprise certificate, making it impossible to install it on an iOS device. The enterprise certificate allowed the Assistenza app to bypass Apple certification and stay accessible for downloads through phishing sites outside the App Store.

An earlier version of the spyware app was discovered on Android last year. The Android version of the app had gained root access to the phones of hundreds of victims – so developers could read Wi-Fi passwords and users' emails as well as data from apps like Facebook, Gmail, WhatsApp, Viber, and WeChat. Lookout also contacted Google last year and worked together to remove the apps from the Play Store.

Both the Android and iOS apps disguised themselves as apps made by Italian and Turkmenistani mobile operators. The apps pretended to be carrier helpline apps that users could install to get in touch with the operators. The real developer was actually Connexxa, a spyware maker.

It's not the only app that has tried to take advantage of such

a loophole. There’s a whole world of illicit apps that use enterprise certificates to fly under Apple’s radar. They offer pirated content, porn, gambling, and all kinds of material that Apple normally wouldn’t allow under App Store guidelines.

Facebook, in particular, first attracted Apple’s attention when it began paying people to install a “Facebook Research” VPN, which siphoned user phone and web data. Google was found to be running a similar program, and in response, Apple briefly revoked the certificate used by Google and Facebook to push updates on their apps. Apple told *Recode* at the time that enterprise certificates were meant “solely for the internal distribution of apps within an organization.”

https://www.theverge.com/2019/4/8/18300822/spyware-app-abused-ios-enterprise-certificate-track-targets