# Phishing Sites Distributing IOS & Android Surveillanceware

By Lookout

Published: 2016-07-15 · Archived: 2026-04-05 12:47:39 UTC

*For the past year, Lookout researchers have been tracking Android and iOS surveillanceware, that can exfiltrate contacts, audio recordings, photos, location, and more from devices. As has been previously reported, some versions of the Android malware were present in the Google Play Store. The iOS versions were available outside the app store, through phishing sites, and abused the Apple Developer Enterprise program.*

## Background: Android surveillanceware

Early last year, Lookout discovered a sophisticated Android surveillanceware agent that appears to have been created for the lawful intercept market. The agent appears to have been under development for at least five years and consists of three stages. First, there is a small dropper, then a large second stage payload that contains multiple binaries (where most of the surveillance functionality is implemented), and finally a third stage which typically uses the DirtyCOW exploit (CVE-2016-5195) to obtain root. Security Without Borders has recently published an analysis of this family, independently, through their blog.

Several technical details indicated that the software was likely the product of a well-funded development effort and aimed at the lawful intercept market. These included the use of certificate pinning and public key encryption for C2 communications, geo-restrictions imposed by the C2 when delivering the second stage, and the comprehensive and well implemented suite of surveillance features.

Early versions of the Android application used infrastructure which belonged to a company named Connexxa S.R.L. and were signed using the name of an engineer who appears to hold equity in Connexxa.

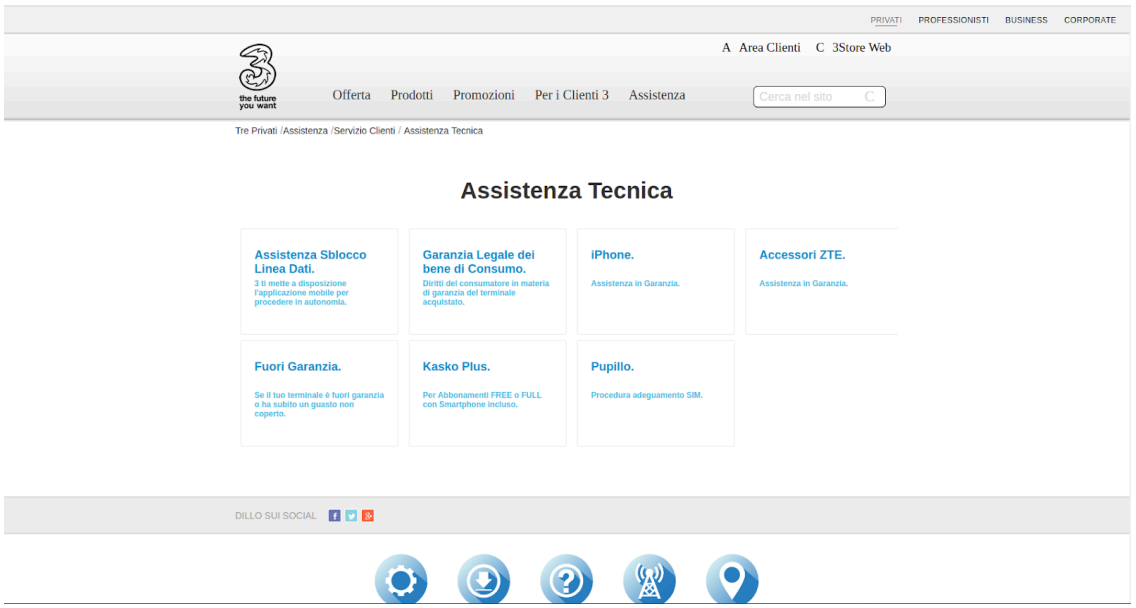
This engineer’s name is also associated with a company called eSurv S.R.L. eSurv’s public marketing is centered around video surveillance software and image recognition systems, but there are a number of individuals claiming to be mobile security researchers working at the company, including one who has publically made claims to be developing a mobile surveillance agent.

Moreover, eSurv was a business unit of Connexxa and was leased to eSurv S.R.L in 2014. This business unit and the eSurv software and brand was sold from Connexxa S.R.L. to eSurv S.R.L. on Feb 28, 2016.

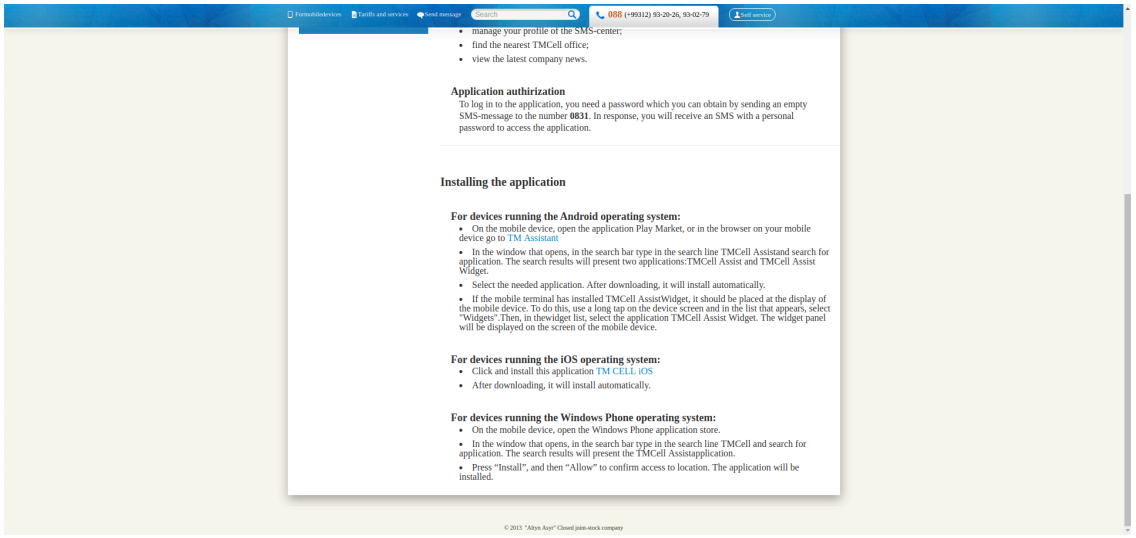
Lookout notified Google of the potential threat shortly after it was discovered. Together, during the latter half of 2018, we worked to remove the apps from the Play store while it was being deployed in the wild.

**iOS development**

Analysis of these Android samples led to the discovery of infrastructure that contained several samples of an iOS port. So far, this software (along with the Android version) has been made available through phishing sites that imitated Italian and Turkmenistani mobile carriers.




*Wind Tre SpA - an Italian telecom operator*

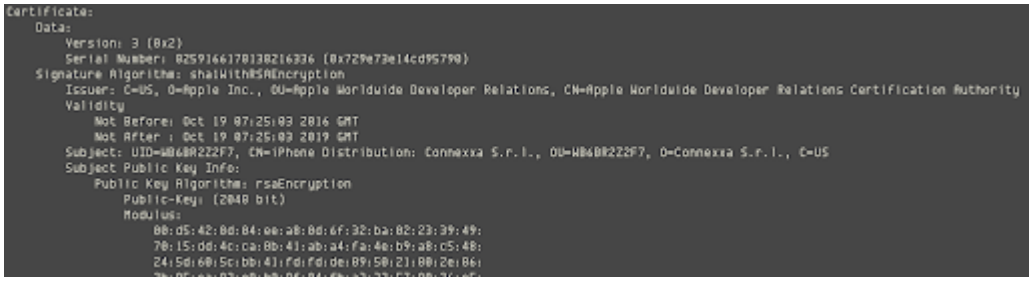



*TMCell - the state owned mobile operator in Turkmenistan*

Deployment to users outside Apple's app store was made possible through abuse of Apple's enterprise provisioning system. The Apple Developer Enterprise program is intended to allow organizations to distribute proprietary, in-house apps to their employees without needing to use the iOS App Store. A business can obtain access to this program only provided they meet requirements set out by Apple. It is not common to use this program to distribute malware, although there have been past cases where malware authors have done so.

Each of the phishing sites contained links to a distribution manifest, which contained metadata such as the application name, version, icon, and a URL for the IPA file.

To be distributed outside the app store, an IPA package must contain a mobile provisioning profile with an enterprise's certificate. All these packages used provisioning profiles with distribution certificates associated with the company Connexxa S.R.L.




*Certificate Used*

The apps themselves pretended to be carrier assistance apps which instructed the user to "*keep the app installed on your device and stay under Wi-Fi coverage to be contacted by one of our operators*".


*One of the packages after initial launch*

The iOS variant is not as sophisticated as the Android version, and contained a subset of the functionality the Android releases offered. In particular, these packages have not been observed to contain or to download exploits which would be required to perform certain types of activities on iOS devices.

Even without capabilities to exploit a device, the packages were able to exfiltrate the following types of data using documented APIs:

- Contacts
- Audio recordings
- Photos
- Videos
- GPS location
- Device information

In addition, the packages offered a feature to perform remote audio recording.

Though different versions of the app vary in structure, malicious code was initialized at application launch without the user's knowledge, and a number of timers were setup to gather and upload data periodically.

Upload data was queued and transmitted via HTTP PUT requests to an endpoint on the C2. The iOS apps leverage the same C2 infrastructure as the Android version and use similar communications protocols. Push notifications were also used to control audio recording.

Lookout has shared information about this family with Apple, and they have revoked the affected certificates. As a result, no new instances of this app can be installed on iOS devices and existing installations can no longer be run. Lookout customers are also protected from this threat on both Android and iOS.

*I will be presenting my findings at the Kaspersky Security Analyst Summit in Singapore this week.*

---