Lookout

THREAT GUIDANCE

ToTok

Overview

Open-source security group Objective-See discovered a massively popular mobile chat app for iOS and Android that was built by the United Arab Emirates to “track every conversation, movement, relationship, appointment, sound and image of those who install it on their phones.” Built on top of Chinese chat app YeeCall, the app didn’t break Apple or Google developer guidelines, asking only permissions available to most developers. That said, the app enables broad surveillance of millions of users around the world. Heavy governmental restrictions on apps like Skype and WhatsApp, drove mobile users in the UAE to download ToTok, which conveniently was both free and more reliable. With unlimited voice and video calling, as well as secure messaging, it was incredibly attractive to millions of Emiratis, and most recently millions of users outside the UAE.

How Does it Work?

ToTok asked for permission to access the microphone, calendar, location, photos, contacts, Siri integration, and camera, which all seemed legitimate since they mirror the permissions of popular chat apps. This demonstrates a new direction for surveillance programs. The app explicitly asks for permissions, but doesn't abuse these permissions, instead it relies on organic user activity in order to achieve their surveillance goals. Using permissions available to iOS and Android developers, ToTok is a good example of how threat actors can leverage mobile devices for unrivaled surveillance programs.

Lookout Recommendation for Admins

Lookout Mobile Endpoint Security enables admins to create more than 55 custom app security policies, allowing organizations to easily create security policies that block the use of apps exhibiting specific behaviors. To prevent users from being exposed to surveillanceware programs like ToTok, Lookout admins can implement a custom app policy to identify and blacklist new, unfamiliar apps that request a significant number of permissions.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout’s global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Lookout Threat Advisory

Lookout

Lookout.com