TikTok Pro

Overview

In June 2020, TikTok was banned from the iOS and Google Play stores in India due to activities "prejudicial to the sovereignty and integrity of India." Just a week later in July, the US Secretary of State announced that the United States was looking into a similar ban over security concerns of the app and the activities of its parent company ByteDance.

Within a week of India banning TikTok, malicious actors started taking advantage of the ban to deliver malware to victims. Maharashtra Cyber, which is a Nodal office under the Government of Maharashtra for Cyber Crime investigation, tweeted out a warning of a fake TikTok Pro app being distributed via SMS, social media, and messaging platforms.

Lookout Analysis

Lookout conducted an in-depth analysis of the fake TikTok Pro app and has classified it as toll fraud malware. Toll fraud is an old but effective way for malicious actors to deliver a cheaply built app (ex: TikTok Pro's file is only 2.2MB versus TikTok, which is 55.2MB on Android) in order to leverage the victim's phone for financial gain.

Lookout found that the malicious app requests very similar permissions as the real TikTok app such as the location, device sensor data, and contacts. The device user installs this app by sideloading it, which means it's installed from a 3rd-party app store. While sideloaded apps are not always intended to be malicious, they can be laced with malware and introduce threats to the user's personal or corporate data accessed from the device. Once TikTok Pro is sideloaded onto the device, it cannot be opened on the device and acts as toll fraud malware that sends premium text messages to Indian phone numbers without the end-user's knowledge.

Lookout and Recommendation for Admins

Lookout warns end users about app risks, including sideloads, on iOS and Android devices as they happen. The Lookout client takes immediate action when it detects an app on the device that doesn't originate from an official app store or an enterprise's own EMM solution. Lookout responds according to the organization's policy by either alerting the user or alerting the user and blocking internet access. This ensures that no corporate data is at risk while the app is on the device. Lookout detects side-loaded apps on both iOS and Android devices, protecting devices in a consistent way independent of the mobile platform.

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