TikTok

Overview

In January 2020, two US military organizations banned TikTok because of communication with servers in China and Russia. Then, in June 2020, India decided to ban TikTok from the iOS and Google Play stores citing 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.

All of this comes on the heels of two reports. The first from an independent researcher who managed to reverse engineer the app and classified it as "a data collection service that is thinly veiled as a social media app" in a highly publicized findings report. The other is an ongoing project by the Australian Strategic Policy Institute (ASPI), which evaluates the "reach" of China's largest technology companies and implicates ByteDance in surveillance work with the Xinjiang Internet Police

Lookout Analysis

Lookout conducted in-depth analysis of the app with its Mobile App Risk Analysis tool to make sure there wasn't any greater danger to TikTok users. We concluded that the servers themselves didn't execute malicious activity, which would have been a signal of direct nefarious activity. However, it's impossible to tell what is being done with data sent over those servers and who has access to users' information. Between January and July, it was notable that the number of IP addresses the iOS app connected to in China was reduced from 119 to 11, but increased from 0 to 5 for the Android app.

Lookout classified the following behaviors by TikTok apps as having elevated risk exposure:

- Monitors location changes
- Accesses the clipboard
- Authorized to access camera
- Executes commands in separate processes
- Accesses the clipboard
- Uses common RNG seed (Android)

Lookout and Recommendation for Admins

TikTok has been banned by India, the US military, and the Australian Defence Force as of July 1st, 2020. Considering the widespread security concerns of the app and its parent company, Lookout Admins should blocklist the app. Lookout enables admins to run risk analyses of any iOS or Android app with our App Analysis tool. Admins will receive a report breaking down all app components, including IP addresses by country used by the app. Armed with this information, Lookout Admins make highly informed decisions about what apps they want to blacklist.

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