Mintegral SDK (SourMint)

Overview

An advertising SDK from Chinese mobile ad platform Mintegral was discovered by security firm Snyk to be active in over 1,200 iOS apps totaling roughly 300 million downloads per month. Dubbed as SourMint by Snyk, the Mintegral SDK contains malicious code that has extensive visibility into PII on your device, sends any URL requests from the app it's integrated in back to a third-party server, and can allegedly report false clicks on ads to steal revenue away from the app developer.

The Mintegral SDK can be easily acquired and integrated into an app just like any other SDK. However, it's been discovered that there is a fair amount of self-obfuscation that occurs if the SDK detects any debugging or proxy tools on the device. By modifying its behavior in the presence of those tools, the SDK can hide its true intent. This also likely helps it pass through Apple's app review process for the iOS App Store.

Lookout Analysis

Lookout researchers have classified the Mintegral SDK as Riskware because of the amount of data it sends from the user device, including information from users within app web navigation such as URL requests and headers, in-app behavior, and other private user data that could be monetized by being sold to other parties for data analytics. Despite the fact that Snyk, Lookout, and others have classified this behavior as malicious, Apple is continuing to allow these apps on the App Store.

Below is a sampling of popular iOS apps with SourMint embedded in them as of January 2021.

Lookout Coverage and Recommendation for Admins

Lookout implemented detection over the air for the initial set of apps known be using the Mintegral SDK shortly after discovery. Any occurrences of apps with the Mintegral SDK will appear in the Apps section of the admin console classified as Riskware. As more apps are discovered to have this SDK, Lookout will continuously implement additional coverage.

Lookout continues to monitor Mintegral SDK releases and will update and adjust coverage when the malicious capabilities are removed. This will ensure that benign versions of previously flagged apps are not classified as Riskware.

Understanding What's Inside

This SDK exemplifies the importance of understanding what mobile apps bring with them when being downloaded to a device. This is particularly difficult for IT, security, and mobility teams to understand if they allow employees to user personal device for work in a bring-your-own-device (BYOD) scenario. Without visibility into those devices and the risks that may lie in personal apps, it's impossible to have an airtight corporate security strategy.

Lookout Mobile Risk & Compliance

Lookout Risk and Compliance provides full visibility into the mobile apps in your organization's fleet and enables you to implement organization-wide governance, risk and compliance policies. Lookout delivers a unique capability to provide mobile application risk assessment that gives the necessary insight into app permission and data access controls. The Lookout Security Graph has aggregated the insight from analyzing more than 120 million apps across nearly 200 million devices.

Click here to learn more about Lookout Mobile Risk and Compliance