Lookout Discovery – BeiTaAd Plugin

Lookout is constantly discovering and researching new threats to protect and advise our customers

Background and discovery timeline

In late 2018, Lookout researchers discovered a well-obfuscated advertising plugin hidden within a number of popular applications in Google Play. The plugin forcibly displays ads on the user's lock screen, triggers video and audio advertisements even while the phone is asleep, and displays out-of-app ads that interfere with a user's interaction with other applications on their device. In total, researchers discovered 307 unique applications that include BeiTaAd, with over 440 million cumulative installations.

Key facts

1. Unique in prevalence and level of obfuscation used to hide existence
2. Works by decrypting hidden file in the app to load and save the plugin
3. Never installed to the device and cannot be uninstalled without removing the infected application

Capabilities and affected parties

This plugin renders phones nearly unusable. The ads do not immediately bombard the user, but become visible about 24 hours after the application is launched, some waiting as long as two weeks after being launched. The plugin has been refactored several times since its initial release in 2018, however the new iterations consist of an AES encrypted dex file disguised as a benign .renc file. Encryption and obfuscation techniques evolved over time to hide the plugin, with strings related to its activity eventually being XOR encrypted and Base64-encoded. When the application is launched, an SDK is initialized that retrieves the asset path where BeiTaAd is located, and checks whether it has been decrypted and loaded before storing it on the device. BeiTaAd is never actually installed on the device, so it cannot be removed without uninstalling the main application that the user initially downloaded. As of May 23rd, 2019, the 230+ affected applications on Google Play have either been removed or updated to versions without the BeiTaAd Plugin.

How Lookout detects and protects against threats like BeiTaAd

In the case of BeiTaAd, the investigation of several applications that were seen displaying full screen ads on the home screen allowed Lookout researchers to uncover the breadth of this plugin and the obfuscation efforts put in over time to keep it hidden. Since starting to detect and alert to BeiTaAd, Lookout has protected hundreds of thousands of devices from the adware. This plugin family provides insight into the future development of mobile adware, and it is likely we'll see other developers attempt to use similar techniques to avoid detection.

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 Threat Advisory