Ghost Push and Gooligan: One and the Same

By Lookout

Published: 2016-12-01 · Archived: 2026-04-02 11:19:23 UTC

You may have seen headlines about a new family of malware called "Gooligan." This is not actually a net new malware family, but rather it's a variant of the family "Ghost Push," a threat first discovered in 2014. Lookout customers have been protected against this threat since then.Google released a blog post on the threat called, "The fight against Ghost Push continues." In it, the company reveals that is has been tracking the malware and acknowledges a problem anyone, especially enterprises, should be watching for: malware evolves and becomes more sophisticated over time.

You’re already protected

Lookout already has coverage for these families and variants.

We encourage Android users to keep their devices up-to-date with the latest security patches (some instances of Gooligan malware attempt to use known vulnerabilities to exploit a device), use caution when downloading apps from third-party stores, and ensure you’re using Lookout to stay ahead of and protected from mobile threats.

What it does

Android devices get infected by Ghost Push when a person installs a malicious app. Once installed, the malware “drops” or installs additional, and sometimes harmful apps on the device. Lookout detects these malware families and variants, as well as the newly-downloaded apps they drop onto the device.

This variant of the malware family is reportedly responsible for compromising one million Google accounts that may include Gmail, Google Play, Google Drive and other account-types. While the claims are no doubt true that Google authorization tokens have been collected, posing a risk to Google accounts, Google has stated they have seen no evidence of user data access or fraudulent activity on the affected accounts.
