Detecting and eliminating Chamois, a fraud botnet on Android

Archived: 2026-04-05 20:11:45 UTC

Posted by Security Software Engineers—Bernhard Grill, Megan Ruthven, and Xin Zhao

Google works hard to protect users across a variety of devices and environments. Part of this work involves defending users against Potentially Harmful Applications (PHAs), an effort that gives us the opportunity to observe various types of threats targeting our ecosystem. For example, our security teams recently discovered and defended users of our ads and Android systems against a new PHA family we've named Chamois.

Chamois is an Android PHA family capable of:

- **Generating invalid traffic** through ad pop ups having deceptive graphics inside the ad
- Performing **artificial app promotion** by automatically installing apps in the background
- Performing **telephony fraud** by sending premium text messages
- Downloading and executing additional plugins

Interference with the ads ecosystem

We detected Chamois during a routine ad traffic quality evaluation. We analyzed malicious apps based on Chamois, and found that they employed several methods to avoid detection and tried to trick users into clicking ads by displaying deceptive graphics. This sometimes resulted in downloading of other apps that commit SMS fraud. So we blocked the Chamois app family using Verify Apps and also kicked out bad actors who were trying to game our ad systems.

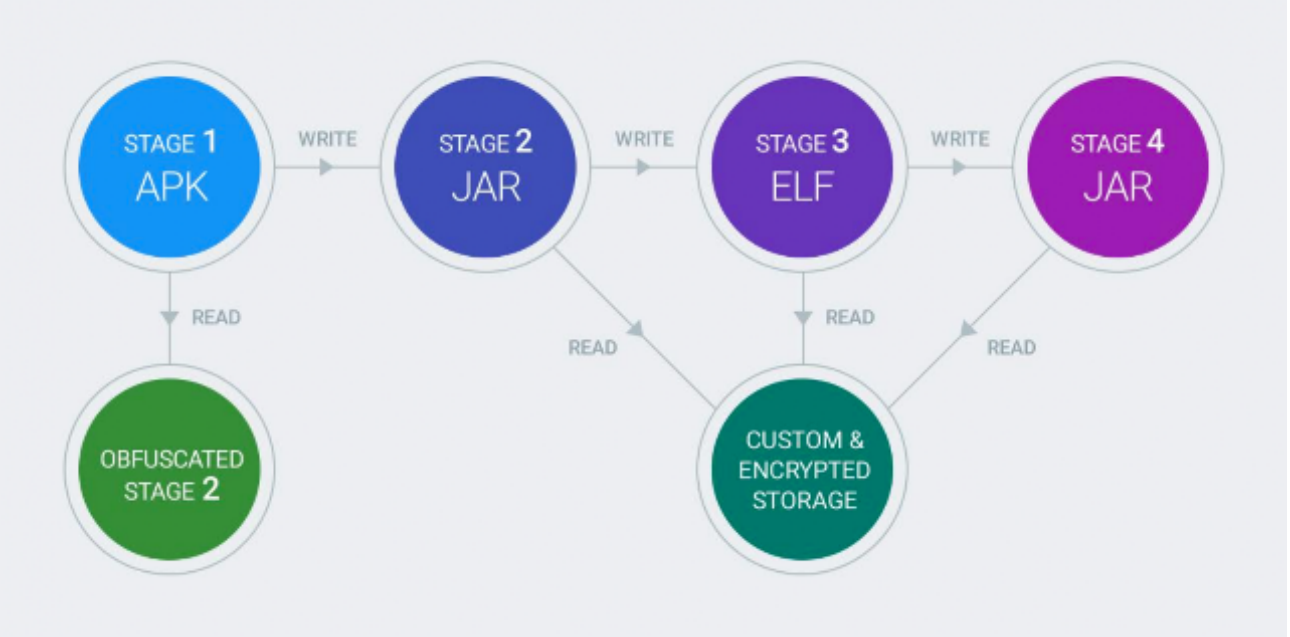
Our previous experience with ad fraud apps like this one enabled our teams to swiftly take action to protect both our advertisers and Android users. Because the malicious app didn't appear in the device's app list, most users wouldn't have seen or known to uninstall the unwanted app. This is why Google's Verify Apps is so valuable, as it helps users discover PHAs and delete them.

Under Chamois's hood

Chamois was one of the largest PHA families seen on Android to date and distributed through multiple channels. To the best of our knowledge Google is the first to publicly identify and track Chamois.

Chamois had a number of features that made it unusual, including:

- **Multi-staged payload**: Its code is executed in 4 distinct stages using different file formats, as outlined in this diagram.



This multi-stage process makes it more complicated to immediately identify apps in this family as a PHA because the layers have to be peeled first to reach the malicious part. However, Google's pipelines weren't tricked as they are designed to tackle these scenarios properly.

- **Self-protection**: Chamois tried to evade detection using obfuscation and anti-analysis techniques, but our systems were able to counter them and detect the apps accordingly.
- **Custom encrypted storage**: The family uses a custom, encrypted file storage for its configuration files and additional code that required deeper analysis to understand the PHA.

- **Size**: Our security teams sifted through more than 100K lines of sophisticated code written by seemingly professional developers. Due to the sheer size of the APK, it took some time to understand Chamois in detail.

Google's approach to fighting PHAs

Verify Apps protects users from known PHAs by warning them when they are downloading an app that is determined to be a PHA, and it also enables users to uninstall the app if it has already been installed. Additionally, Verify Apps monitors the state of the Android ecosystem for anomalies and investigates the ones that it finds. It also helps finding unknown PHAs through behavior analysis on devices. For example, many apps downloaded by Chamois were highly ranked by the DOI scorer. We have implemented rules in Verify Apps to protect users against Chamois.

Google continues to significantly invest in its counter-abuse technologies for Android and its ad systems, and we're proud of the work that many teams do behind the scenes to fight PHAs like Chamois.

We hope this summary provides insight into the growing complexity of Android botnets. To learn more about Google's anti-PHA efforts and further ameliorate the risks they pose to users, devices, and ad systems, keep an eye open for the upcoming "Android Security 2016 Year In Review" report.
