# Hugely Popular Android Apps Have Been Committing Ad Fraud Behind Users Backs To Help Google Spy On You

“Why isn't Google immediately dropping such apps from the Play Store and advising users to uninstall them?” one analyst asked.


**Craig Silverman**

- Tweet
- Share

- Copy

**Eight apps with** a total of more than 2 billion downloads in the Google Play store have been exploiting user permissions as part of an ad fraud scheme that could have stolen millions of dollars, according to research from Kochava, an app analytics and attribution company that detected the scheme and shared its findings with BuzzFeed News.

Seven of the apps Kochava found engaging in this behavior are owned by Cheetah Mobile, a Chinese company listed on the New York Stock Exchange that last year was accused of fraudulent business practices by a short-seller investment firm — a charge that Cheetah vigorously denied. The other app is owned by Kika Tech, a Chinese company now headquartered in Silicon Valley that received a significant investment from Cheetah in 2016. The companies claim more than 700 million active users per month for their mobile apps.

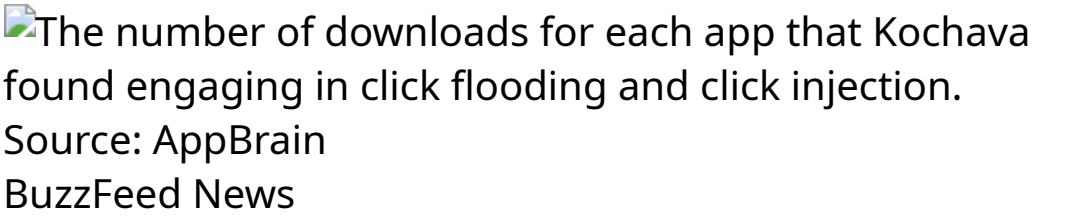
The allegations are the latest shock to a vast digital ad tech industry that remains dogged by a multibillion-dollar fraud problem and a mobile ecosystem rife with malicious ads and fraudulent practices. BuzzFeed News reported last month on an ad fraud scheme that tracked user behavior in dozens of Android apps to generate fake traffic and steal advertisers' money. Google estimated close to $10 million was stolen from it and its partners, and subsequently removed many of the apps from its Play store.

While the most immediate victims are brands who lose ad dollars to bots and other schemes, ad fraud also diverts revenue away from legitimate publishers and developers. In the case of mobile apps, it can cause frustration for users who may see their phone battery drained and data usage spike as a result of illegitimate ad transactions taking place without their knowledge.

This particular scheme exploits the fact that many app developers pay a fee, or bounty, that typically ranges from 50 cents to $3 to partners that help drive new installations of their apps. Kochava found that the Cheetah and Kika apps tracked when users downloaded new apps and used this data to inappropriately claim credit for having caused the download. The practice being executed by Cheetah and Kika is referred to as click flooding and click injection, and ensures these companies are rewarded an app-install bounty even when they played no role in an app's installation. (See “How It Works” below for a detailed description.)

“This is theft — no other way to say it,” Grant Simmons, the head of client analytics for Kochava, told BuzzFeed News. He said this example is notable because Cheetah Mobile and Kika Tech are large app developers that built these practices into their apps.

“These are real companies doing it — at scale — not some random person in their basement,” he said.


The number of downloads for each app that Kochava found engaging in click flooding and click injection.
Source: AppBrain
BuzzFeed News

The number of downloads for each app that Kochava found engaging in click flooding and click injection.
*Source: AppBrain*

After being sent a video captured by Kochava of the Kika Keyboard app engaging in click injection and click flooding, Kika Tech's US general manager, Marc Richardson, said the company "has no intentions of engaging in fraudulent practices."

"Kika Keyboard is a large, well-known app that helps its users communicate in many unique ways and we are extremely disappointed to learn about these 'flooding and injection' practices. We appreciate you putting this to our attention," he said.

Kika also provided BuzzFeed News with a statement from CEO Bill Hu suggesting that any ad fraud took place without the company's full knowledge.

"At this time, Kika is extensively researching the critical issues you raised internally. If in fact, code has been placed inside our product we will do everything to quickly and fully rectify the

situation and take action against those involved," he said. "For now, we do not have further comments as we begin our internal research."

But Kochava and an additional analysis by Praneet Sharma of Method Media Intelligence for BuzzFeed News both found that the Kika Keyboard app executed click flooding and injection using the company's own proprietary software and with functions built directly into the app itself. "No one got in there and fiddled with anything," Simmons said.

He said he's seen other apps run by Chinese companies engage in this same conduct: "It's not as if it's some big state secret. It's more that this is the de facto business tactic given the app universe, especially in China."

Cheetah Mobile issued a statement to BuzzFeed News that suggested third-party software development kits, or SDKs, integrated into its apps were responsible for the click injection.

"We work with many mainstream ad platforms via SDK integration. We request ads via SDK from these ad platforms and display their ads. We have no control over the behavior of these SDKs," said a statement emailed from a spokesperson. "Ad platforms and independent arbitration parties work together to decide attribution of app installations, and we are not part of that process. We are continuing to look into the matter and will update you if we have any further information."

However, the SDK involved in the suspect activity is actually owned and developed by Cheetah, not by third parties, according to Kochava. When sent that information by BuzzFeed

News, Cheetah said that "none of Cheetah Mobile's SDKs are involved in click injection."

Simmons said, "If what we have discovered and documented is not fraud, we'd be very curious to hear an explanation of what it is." (Cheetah and Kika were Kochava customers at the time Simmons and his team discovered the click injection and click flooding taking place.)

Along with raising serious questions about the business practices of two prominent Chinese app developers, this highlights the security, privacy, and ad fraud issues in the Android app ecosystem and Google Play store. BuzzFeed News provided Google with videos of the Cheetah and Kika apps captured by Kochava, as well as with screenshots of relevant app code identified by Method Media Intelligence. Google initially said it had not confirmed the presence of fraudulent tactics in the apps, and that it has asked for additional information from Kika and Cheetah. It told BuzzFeed News it continues to investigate.

"Google is the curated owner of the Google Play store and the owner of one of the largest monetization mechanisms for apps. If there is confusion on where ad fraud and attribution fraud is taking place in this ecosystem, we'd be happy to help Google in their efforts," Simmons said.

Richard Kramer, a senior analyst with Arete, an independent research firm that covers mobile and technology companies, said Google needs to remove the affected apps from its Play store.

“Why isn't Google immediately dropping such apps from the Play store and advising users to uninstall them?” he told BuzzFeed News. “It may reduce [ad] inventory in their Network, but I would expect [Google] to be more sensitive to quality of impressions.”

“The entire industry needs to do more than hide behind plausible deniability,” he added.

The problem of app-install fraud is widespread. App installs are a more than $7 billion global market, according to eMarketer. AppsFlyer, an app attribution platform, analyzed 1 billion app installs over the past 12 months and found 25% were fraudulent, which means an estimated $1.7 billion was stolen in the past year.

Uber is currently suing one of its ad agencies for, among other things, “fraudulently claiming credit for app downloads that happened without a customer ever clicking on an ad.” The agency in question denies the accusation.

# “Wildly Over-Permissioned”

The Cheetah apps implicated are Clean Master, CM File Manager, CM Launcher 3D, Security Master, Battery Doctor, CM Locker, and Cheetah Keyboard. Several are among the most popular productivity apps in the entire Google Play store. Just in the past 30 days, these apps were downloaded more than 20 million times, according to data from the AppBrain analytics service. CM Launcher 3D is also promoted to users as one of Google Play’s “go-to apps."

In its latest quarterly earnings, Cheetah reported that it brought in $196 million in revenue from “utility products and related services,” of which these seven apps are a key component. Utility products generated roughly half of the company’s total revenue last quarter. (Cheetah does not break out revenue by advertising type, so it’s not possible to know how much was generated by app install claims.)

The other app that engaged in a similar practice is Kika Keyboard, which enables users to send a wide range of emojis. It’s the most popular keyboard in the Google Play store and claims to have 60 million monthly active users.

The affected Cheetah and Kika apps require users to give a wide range of permissions, including the ability to track keystrokes or see when other apps are downloaded, which raises questions about the amount of data collected by these companies, according to Sharma, CTO of the ad fraud investigation firm Method Media Intelligence. He described the apps as “wildly over-permissioned.”

“The fact that you have such high-permissions apps, you’ve got apps from companies that are based in China and they collect so much information,” Sharma said. “They are logging everything, so … from a privacy standpoint they are violating a lot of things.”

Richardson of Kika said the company takes “data security very seriously and it’s at the very core of what we do. Our data collection and usage has always been strictly in line with Google’s policies and the GDPR laws.”

Sharma says Google and other companies that operate app stores shouldn’t accept apps that require such a high level of permissions.

“There is very little monitoring and security” in the Android ecosystem, he said.

# How It Works

App developers often issue so-called bounties for third parties to help drive installations. If a user clicks on an ad for an app and then installs and opens it, the app's developer will pay the ad network. The key is to know who should get credit for driving that installation, as the money needs to flow to the network that served the ad, as well as to the publisher of the app or website where the ad appeared, for example. This is the weakness in the system. App install attribution, as it's called, is often not an exact science because it can be hard to definitively identify which ad led to the installation of an app on a specific phone.

To attribute the installation to the correct party, information about the device used to click on the ad and the network and publisher that served it is passed along with the app installation. When the app is finally opened, the app does a "lookback" to see where the last click came from and attribute the installation accordingly.

Kochava found that Cheetah and Kika apps are gaming this attribution system to ensure they're awarded the last click. This is true even in cases when no ad was served and they played no role in the installation.

"At no point do the involved publishers add marketing value" to the app installations, Simmons said.

BuzzFeed News

# Cheetah Mobile Apps

Kochava identified seven Cheetah apps that require users to give them permission to see when new apps are downloaded, and to be able to launch other apps. The Cheetah apps listen for when a user downloads a new app. As soon as a new download is detected, the Cheetah app looks for active install bounties available for the app in question. It then sends off clicks that contain the relevant app attribution information to ensure Cheetah wins the bounty — even though it had nothing to do with the app being downloaded. This is referred to as click injection.

As an extra piece of insurance, Simmons says Cheetah's apps are also programmed to launch the newly downloaded app without the user's knowledge. This helps increase the odds that it will receive credit for the app install, as the bounty is only paid when a user opens a new app.

"The nefarious tactic attempts to open the app automatically because it ensures credit can be claimed against the fraudulent click."

## Kika Keyboard

Kika Keyboard is uniquely positioned to execute both click flooding and click injection. As a keyboard, it requires users to give it permission to see what's being typed. The Kika app uses this to listen for any Play store searches a user makes for other apps. The Kika Keyboard then begins looking for install bounties on offer for apps related to those searches, according to Kochava's findings. Once it identifies apps with offers, Kika generates a series of clicks with attribution information contained in them in an attempt to claim the bounty on any future installations related to the users' app searches.

The app also listens for app store searches even when Kika Keyboard is not active, something Simmons said was particularly concerning. As in the above example, it listens for what a user searches for in the app store. But rather than firing attribution clicks right away, it will display ads for apps with active offers, Kochava found. If the user were to download an app as part of this search session, Kika would claim credit for it, even though the user never actually clicked on an ad to generate the installation.

"They're going to place as many bets across as many apps that you may be interested in," Simmons said.

The final piece involves obscuring the fact that the Cheetah and Kika apps are involved in such a high number of app installations. Simmons said the Cheetah and Kika apps are loaded with proprietary software to facilitate and conceal app attribution. This enables them to pass the attribution through

many ad networks to hide the fact that so many attribution wins are coming from these apps.

Simmons said Kochava found that Kika Keyboard and just one of the Cheetah apps spread install attribution claims across more than 20 ad networks. Kochava also found they sometimes use fake app names to further obscure the role that the Kika and Cheetah apps played.

“The injected clicks are reported from many different ad networks, and the sub publishers within those networks are either a lie or obscured,” he said.

"What we’ve discovered traces the source back to the apps referenced and demonstrates it — we’re not sure how a reasonable person could conclude the behavior is legitimate." ●

**App Ad Fraud**

- Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme Craig Silverman · Oct. 23, 2018
- Sen. Mark Warner Is Pressing The FTC To Tackle Digital Ad Fraud After A BuzzFeed News Investigation Craig Silverman · Oct. 25, 2018
- This Ad Fraud Scheme Stole Millions, But Almost No One Wants To Own Up To It Craig Silverman · Oct. 31, 2018