Click injections explained

Mobile user acquisition fraud in 2017

Fraud affects mobile app marketers not only by siphoning off marketing budget, but also by undermining the accuracy of marketing analytics.

Click injection is a new type of mobile user acquisition fraud. Profiled as the upcoming threat in 2017, our analysts have been researching click injections for the past few months.

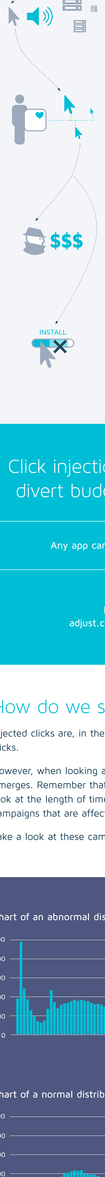
But what is it exactly, and how does it work?

How does it work?

A fraudulent app developer can release a "fraudulent app", which generates advertising revenue for the developer by faking response to advertising campaigns.

The fraudster employs "install broadcasts" to spoof a well-timed click just as a user downloads an app, so that the user appears to have installed the app after having clicked an ad in the fraudulent app.

Here's how it would go down:



John has a fraudulent app installed on his device – usually a simple, free app with some ads, like a solitaire game or a "flashlight".

When John downloads a new app to his device, every other installed app is informed about the download through Android "install broadcasts".

The fraudulent app notices the download. If the new app has been advertised with display advertising, there's a chance that the fraudulent app has participated in the campaign – and so has access to the tracking codes.

With the tracking codes, the fraudulent app reports a click from John to ad networks and tracking services.

When John then opens the new app for the first time, various analytics services are informed, and start cross-referencing advertising clicks from earlier. This can be a long time after the download was completed!

The legitimate-looking click matches John's device ID perfectly, and his install is attributed to the fraudulent developer – so the fraudster receives a payout that can typically range between $1 to $5.

When the advertiser reviews the performance of their advertising campaigns, more installs appear to be generated by advertising than by organic activity.

Click injections lead advertisers to divert budget to bad campaigns

Any app can "listen in" on these broadcasts.

Read the full story at
adjust.com/click-injection-explained

How do we stop it?

Injected clicks are, in themselves, impossible to distinguish from real clicks.

However, when looking at ad campaigns as a whole, a pattern emerges. Remember that timing is crucial to click injections. So if we look at the length of time between clicks and installs, we can identify campaigns that are affected.

Take a look at these campaigns side by side:

Chart of an abnormal distribution

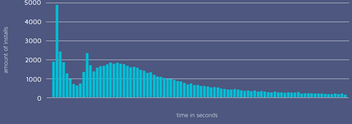
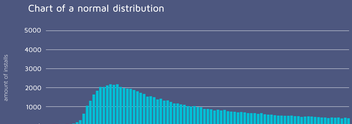


Chart of a normal distribution



Click injections will cause a visible bump in the very early side of the spectrum, where the click happens very shortly before the install. So we can visually spot a problematic campaign when looking at the big picture.

Can we just truncate these quick clicks, then?

It seems intuitive, but not every click that happens shortly before the install is fraudulent. Many clicks are communicated later than they happen (e.g. server-to-server), causing them to have a shorter time-to-install.

Removing those outright causes the same big inaccuracies as we had in the first place.

Preventing mobile advertising fraud – and cleaning up dirty data – is a complex job. To dig deeper into click injection and related forms of user acquisition fraud, read further on our blog:

adjust.com/click-injection-explained