Luxury Daily®

The News and Intelligence You Need on Luxury

COLUMNS

Cat-and-mouse game of mobile ad fraud has only just begun

April 28, 2016

Amit Joshi is director of product and data science at Forensiq

By Amit Joshi

Though mobile advertising has grown to become a $100 billion spending category, we are still very much in the early stages of the fight against mobile ad fraud.

Much like the desktop space back in 2013, advertisers and brands are either unaware of the risks they face or unsure of how to address them.

Fraudsters, as always, are ahead of the curve and continuously finding new ways to game the system.

Last summer, we discovered a set of applications that were leveraging real devices to commit fraud by rapidly refreshing ads that were hidden from the user, a new type of fraud we call mobile device hijacking.

For marketers, there is both good news and bad news.

The good news is that there are many ways that marketers can combat mobile ad fraud. This process begins with understanding the different types of fraud.

The bad news is that as advertisers have started to become aware of ad fraud, fraudsters have already begun implementing more sophisticated methodologies. On both sides of the ecosystem the game has only just begun.

How fraudsters steal credit for legitimate app downloads
Within the cost-per-install (CPI) space we have seen the emergence of a new type of fraud: mobile attribution fraud.

Attribution fraud occurs when fraudsters hijack ad dollars by claiming responsibility for an app download from a user who actually converted organically.

These users behave like typical organic users, and because most advertisers are optimizing on installs, this sort of fraud will go undetected.

For black hats, attribution fraud is low-hanging fruit because they only have to spoof a single data point of data: the click. This can be accomplished in a variety of ways including:

Click spoofing (completely faked server side reported clicks)

Selling impressions as clicks

Hidden clicks generated in the background of mobile Web pages and in-app

We have already started to see these bad actors make clever improvements to mask what they are doing.

Some have sought to confuse advertisers by mixing legitimate and misattributed installs. Others are identifying which advertisers buy space on a certain domain or app, and then fake or force clicks, specifically from visitors.

However, of even greater concern is the fact that still other fraudsters have begun to move to even more advanced types of fraud.

Next evolution of cost-per-install fraud
The newest wave of CPI fraud is install fraud, or fake installs where there is either no real-user or no intent behind the install.

To fake an install, fraudsters use either a real smartphone or an emulator to continuously install and delete the same app over and over again.

This requires the fraudster to fool the advertiser into thinking installs are coming from multiple users, most commonly by resetting either the IDFA or Android ID.

More complex schemes will also leverage proxies to geo-mask location and impersonate United States users even though this kind of fraud is often carried out in India, China and Southeast Asia.

Because these methodologies are more complex, they are also require advanced methodologies to detect.

IN THE BURGEONING CPI space, we are seeing the same pattern that was playing out in the performance marketing ecosystem.

Every new capability developed by anti-fraud vendors is followed by a move from fraudsters to create new methodologies that are ever more difficult for us to detect.

Though it is always going to be a challenge for marketers to keep up with the latest threats, they can go a long way toward protecting themselves by working with an anti-fraud vendor and by thoroughly vetting all of the traffic sources with which they work.

Indeed, while the fight against mobile ad fraud is only just getting started, we have no doubt that with hard work and constant vigilance, the good guys will win in the end.

Amit Joshi is director of product and data science at Forensiq, New York. Reach him at ajoshi@forensiq.com.