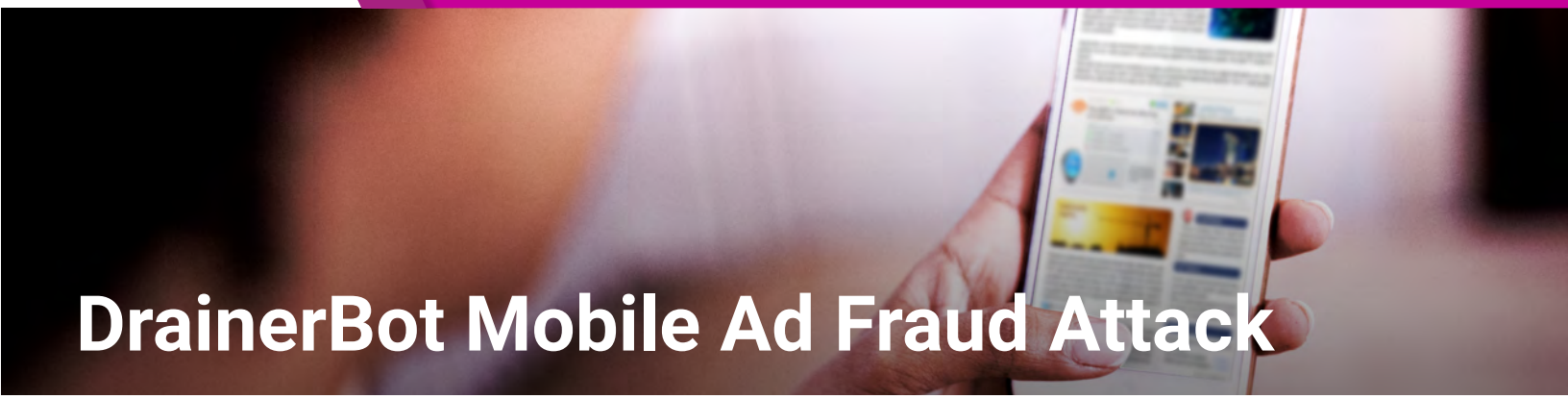
DoubleVerify

FRAUDLAB
FLASH REPORT



DrainerBot Mobile Ad Fraud Attack

Initial analysis of the limited information released by Oracle indicates that most of the fraudulent activity in the DrainerBot attack was previously identified by DV, and that clients employing DV's fraud/SIVT solution were fully covered. The DV Fraud Lab has analyzed both the apps and the SDK (Tapcore) highlighted in the Oracle release to deconstruct the specific ways in which this attack was perpetrated, and to confirm our clients were not impacted prior to the announcement.

As part of its standard detection methods, DV applies two overlapping layers of protection to cover the widest range of mobile fraud methods and schemes, ensuring both the apps and devices generating fraudulent activity are identified. For example, one of the fraudulent apps mentioned in the press coverage and previously identified by DV as fraudulent had over 60% of its impressions flagged by DV's device-level detection technology, in addition to the app itself being identified as invalid.

With respect to this purportedly "new" fraud ring, DV identified abnormal traffic patterns across multiple apps going back to Q3 2018. We immediately initiated an investigation of the apps and flagged several of them as fraudulent. The Fraud Lab also reverse engineered several of the apps to discern that, in some cases, developers had implemented the Tapcore SDK in a way that potentially facilitated fraudulent, hidden ad impressions.

" DoubleVerify has been a longtime TAG member and leader in the anti-fraud effort. It is not surprising that they previously detected this suspicious activity and have been working to protect their clients and the industry at large from these types of threats. "

- Mike Zaneis, CEO, TAG

Some of the Tactics Used in a Nefarious Implementation of the SDK Include:

1. A "cooldown"/"timebomb" period before the SDK is activated (used to help evade detection)
2. Excessive permissions needed to run ads when the app is not active by using the SYSTEM_ALERT_WINDOW, for which the Android Developer Guide specifically warns that "Very few apps should use this permission; these windows are intended for system-level interaction with the user"

Specifically for the apps highlighted in the press release, DV previously classified the apps that had material traffic (defined as at least 10k monthly impressions for the purposes of this analysis) as early as September 2018. Apps already classified by DV as Ad Impression Fraud include: "Perfect365", "Draw Clash of Clans", and "Touch 'n' Beat – Cinema".

It should be noted that the DV Fraud Lab undertakes investigations such as this on a regular basis, as a routine part of business. There was nothing particularly new or noteworthy about the methods or exploits utilized by DrainerBot to generate fraudulent mobile ad impressions. In such circumstances, where there is nothing unique to report concerning the fraud (i.e., it is part of our standard protection and does not represent a new type of fraud), DV simply integrates protection into our services without promoting the continuously evolving fraud protection that we provide.

DoubleVerify is one of a limited number of companies whose methods and measurements are accredited by the MRC for Mobile Fraud/SIVT identification. We are proud to report that, based on the information thus far released on DrainerBot, our pre-bid avoidance, real-time blocking and monitoring solutions have been protecting DV customers against this fraud scheme for months. DoubleVerify will continue to review any newly released information on this scheme and will update our assessment, as warranted.