October 14, 2020

Kubient Discovers New "Weasel" Injection Ad Fraud Scheme and Announces Public Availability of Proprietary Pre-Bid AI

KAI uncovers fake traffic being purchased by major DSPs and SSPs

NEW YORK, Oct. 14, 2020 /PRNewswire/ -- Today,Kubient, Inc. (NasdaqCM: KBNT, KBNTW) ("Kubient" or the "Company"), the cloud advertising marketplace that enables advertisers and publishers to reach, monetize and connect their audiences efficiently and effectively, announced its latest findings of fraudulent activity occurring within the programmatic ecosystem. Via its patent pending Kubient Artificial Intelligence (KAI) ad fraud prevention, now available to the public, Kubient detected Wease.IM, a scheme that was duping brands and their supply- and demand- side platforms into purchasing fake traffic. Index Exchange, PubMatic, Sovrn, Verizon Media, Improve Digital, The Trade Desk, Amazon.com, Adobe, Outbrain, Sephora were all victims.

The KAI pre-bid ad-fraud prevention tool helps stop fraud before it happens through pattern recognition and device scoring. The algorithm is trained to analyze the behavior, consistency, and quality to determine its credibility - accurately flagging fraud in less than 10ms of an ad bid, faster than any other tool on the market. In its work with its partners, the KAI team found the Weasel Injection structure and tested it independently. Ultimately, they determined it utilized PreBid.js header bidding but masked/spoofed the true identity of the properties it was selling while also being compliant with both ads.txt and sellers.json protocols. This was accomplished using a bait and switch advert (Malvertising) that when activated would facilitate the Fraudulent Reselling Scheme.

Since 2019, there has been a massive increase in PreBid.js being used to run secondary auctions within display ad units. While some companies defend this behavior by claiming they provide content in the ad unit as well as ads, others like Wease.IM use it in far more nefarious ways. The fraud committed was very simple and effective, and despite seeing other fraud prevention vendors' prebid wrappers existing in the calls, none of them prevented the sale of the traffic. This fraud shows the limits of not only traditional prebid fraud prevention, but also ads.txt and sellers.json.

"We recommend the industry take a hard stance on PreBid.JS resellers and block or ban any such company who engages in it," said Peter Bordes, CEO of Kubient. "Our KAI

technology is diligently tracking, identifying and flagging these bad actors before they siphon more money away from advertisers."

It is estimated that the advertising industry lost $23 billion to digital fraud in 2019. Kubient advises that all publishers monitor their properties and immediately request any advertisers who inject PreBid.js into their ad units to be blocked and only allow buyers to purchase inventory through non-injected PreBid.JS or similar technology that is owned, controlled or managed by the Publishers or their authorized representative.

KAI is now available as a tool for DSPs and SSPs. To learn more about Kubient and its proprietary solutions, visit www.kubient.com.

About Kubient

Kubient is an open marketplace that enables advertisers and publishers to reach, monetize and connect their audiences efficiently and effectively. Through its Audience Cloud, Kubient activates its set of tools to optimize the supply path, eliminate redundancy, stop fraud before it happens.

Media Contract:
Molly Gagnon
kubient@clarity.pr

SOURCE Kubient