Ad Fraudsters Are Becoming More Sophisticated

New tactics are finding traction

ARTICLE | **DECEMBER 06, 2018**

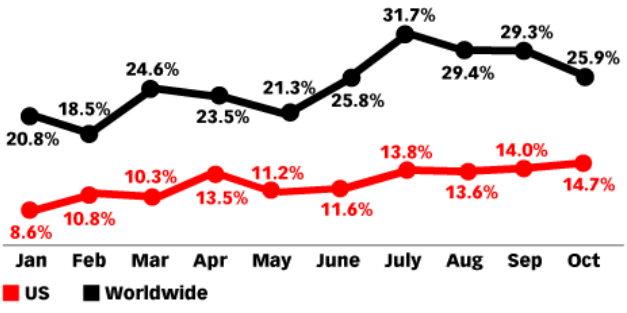
Ross Benes

- A few weeks ago, the FBI announced that it had worked with several companies in the ad industry to dismantle a massive ad fraud operation.
- The fraudsters infected the computers of at least 1.7 million people.
- Aside from deploying bots, the fraudsters used tactics such as tag evasion.
- The multilayered, sophisticated approach the fraudsters took highlights the cat-and-mouse problem of policing ad fraud.

Working alongside tech firms such as Google and White Ops, the US Department of Justice recently took down an ad fraud operation and arrested a few people. While the crackdown may signal that law enforcement agencies are finally taking ad fraud more seriously, it's worth noting that this is just a single bust. The amount of ad fraud in the marketplace is still massive.

Fraudsters often capitalize on changing media consumption patterns. According to Adjust, mobile ad fraud rates have soared as people spend more time on their phones. AppsFlyer analyzed 17 billion app installs across 7,000 apps worldwide over the past 12 months and found that the amount of install fraud in the US keeps increasing.

Mobile App Install Fraud Rate in the US and Worldwide, Jan-Oct 2018
% of total paid app installs



Note: represents activity tracked by AppsFlyer, broader industry metrics may vary
Source: AppsFlyer, Nov 2018
243153 www.eMarketer.com

Tamer Hassan, co-founder and CTO of White Ops, spoke to eMarketer about the evolving tactics used by ad fraudsters to siphon money.

Regarding this recent ad fraud takedown, what tactics stood out to you?

They were basically hijacking IP addresses at corporations and redirecting them to their own servers.

Is that a common tactic?

We've seen it a lot in the old days of email spam, but we hadn't seen it at this scale in ad fraud. It's something newer. It ended up being about 1.7 million IP addresses, corporations of US companies and companies abroad, where they had IP space they weren't using; they were hijacked, taken control of and redirected to [the fraudsters'] bot farms in their data center.

How do fraudsters take over a company's IP addresses?

Basically, a lot of companies have acquired IP space. They don't use it all, and some of it is lying dormant and not assigned. It doesn't have a route on the internet. If there's nobody announcing a set of IPs, and you're able to identify that, you can take over that IP space and redirect it.

What was another tactic the fraudsters used?

Tag evasion. It is a behavior built into the bot to look for a verification tag and suppress it. We're seeing that more and more. We've been watching the behavior for years, but this operation was probably one of the first ones to bring it to scale.

While it's understood why some people are excited that a few fraudsters were arrested, the overall ad fraud economy will keep churning. How can the ad industry adjust its incentives to shut out fraud?

We're used to playing cat and mouse, and we've been talking about this for awhile as an industry. With strategy, we've always said it's economic warfare. It's raising the risk model and lowering the opportunities for profit. The moment [fraud] becomes less attractive—where the losses hurt more than the gains—then you've changed it for all the attackers, rather than trying to just pick off attacker after attacker.