EINPRESSWIRE

Cybersecurity firm Polygraph warns advertisers not to rely on IP blocking to prevent click fraud

IP blocking offers little to no protection against real-world click fraud

BERLIN, GERMANY, July 15, 2022 /EINPresswire.com/ -- Click fraud is a massive problem, stealing tens of billions of dollars from advertisers every year. The fraudsters responsible for this crime include technically savvy website owners, transnational organized crime gangs, and even Nasdaq listed multinationals.

The scam works like this: criminals create websites, and contact advertising networks like Microsoft Ads to request a “publisher advertising account”. Publisher advertising accounts enable the fraudsters to place other company’s ads on their websites, with small fees earned every time the ads are clicked. To ensure maximum profits, the criminals create “bots” – software pretending to be human – and send them to their websites to click on the ads thousands of times per day. For each of these clicks, the advertisers pay money to the ad networks, which is then shared with the criminals.

What makes this crime extra devious are the efforts taken by the fraudsters to remain undetected. One of the tricks they use is ensuring their bots use different IP addresses every time an ad is clicked. To achieve this, they use “residential proxy” services to route the bots’ traffic through random internet users’ home internet connections, effectively randomizing the bots’ IP addresses, and making the clicks look like they came from normal internet users.

According to Trey Vanes, Chief Marketing Officer at cybersecurity firm Polygraph, this laundering of IP addresses makes click fraud detection more difficult. “A common misconception amongst advertisers is that blocking specific IP addresses from seeing or clicking on their ads will prevent click fraud. The problem with this logic is it ignores the reality that most click fraud uses unique IP addresses for each click. That means even if you block the IP addresses which have been used to commit click fraud in the past, it’s not going to make much difference, as those IP addresses are unlikely to be used for click fraud in the future. By using unique IP addresses for every ad click, the criminals ensure blocking IP addresses won’t stop click fraud.”

Vanes believes a different tactic is required to prevent click fraud. “Polygraph monitors the activities of click fraud gangs, so we understand the reality of click fraud and how to stop it. We use a highly effective five-pronged strategy for eliminating fake clicks.

“The first thing to understand is click fraud isn’t random. The fraudsters target high paying ad keywords, as clicks on those ads earn the most money. Polygraph monitors the keywords being targeted by click fraud gangs, so we know which advertisers’ keywords are at risk. Our customers simply remove those keywords from their ad campaigns to avoid click fraud.

“Polygraph keeps track of the websites generating the fake clicks. We provide this list to our customers so they can ban those websites from being able to see or click on their ads. This blocks click fraud at the source, resulting in drastically lower numbers of fraudulent clicks.

“To empower our customers to get click fraud refunds from the ad networks, we provide the details of every fake click, including the dates and times, which IP addresses were used, and why the clicks are fraudulent. Advertisers then give this information to the ad networks and get refunds for their wasted ad spend.

“We give a breakdown of the click fraud coming from each ad network, so our customers can reduce their spend at the ad networks who allow or do a poor job at preventing click fraud.

“Finally, Polygraph uses advanced click fraud detection to ensure even the most sophisticated bots are caught. Our customers are always shocked by the amount of click fraud we’re able to detect – and how much of it the ad networks are missing,” said Vanes.

Polygraph provides an IP blocking service should advertisers still want it. “Of course, if advertisers insist on blocking IPs, we provide that service, but we recommend advertisers focus on removing at risk keywords, block click fraud websites from seeing their ads, and aggressively seek refunds from the ad networks. Polygraph makes this easy,” added Vanes.

For more information, please visit https://polygraph.net

Trey Vanes
Polygraph
+49 160 98058592
email us here