EINPRESSWIRE

Click Fraud Protection Firm Polygraph Advises Advertisers To Check The Source Of Every Ad Click

Criminals are hiding the source of their fake clicks by manipulating the website referrer

BERLIN, GERMANY, August 3, 2022 /EINPresswire.com/ -- Click fraud is the multi-billion dollar crime most people have never heard of. Every year it steals tens of billions of dollars from advertisers, and its culprits include organized crime gangs and Nasdaq listed multinationals.

Most websites earn money through advertising: visitors go to websites and click on the ads scattered throughout the content. For each of these clicks, the advertisers pay fees to an advertising network like Microsoft Ads, and the advertising network shares the money with the website owners.

Criminals are taking advantage of this revenue model by using bots - software pretending to be regular internet users - to generate massive amounts of fake clicks on online advertisements. The bots go to the criminals' websites, click on the ads, and in general try to act like a normal website visitor. The bots repeat this cycle millions of times per day, decimating the advertisers' budgets and earning millions for the fraudsters.

According to Trey Vanes, chief marketing officer at click fraud protection company Polygraph, criminals are trying to hide the source of their fake clicks in a futile attempt to remain undetected.

"Polygraph monitors the activities of click fraud gangs, so we understand their techniques and how to detect them," said Vanes. "The criminals go to great lengths to make their bots look real, tricking the advertising networks into thinking everything is normal, however we're able to see exactly what they're doing.

"When a person - or bot - clicks on an advert, we can see which website displayed the ad before it was clicked. This is known as the website referrer, and it allows us to see the source of every click. This creates a problem for click fraudsters, as it makes it easy for us to identify their scam websites.

"Since their bots are generating millions of clicks each day, we're able to see where these fake clicks are coming from. In other words, we can see which websites are owned by the criminals,

and report them to the ad networks to get them taken down.

"What the criminals are doing now - in an attempt to remain undetected - is delete the website referrer whenever their bots click on an ad. Their thinking is we won't be able to see the source of the clicks, which means their websites will remain a secret, but actually it just makes their fake clicks even more obvious. What we're seeing now is millions of bot clicks with the website referrer set to a blank value. They may as well add a note saying their clicks are fake - it's that obvious."

Vanes advises advertisers to seek refunds from the advertising networks if they notice ad clicks where the source of the click - the website referrer - is blank. "These clicks are 100% fraudulent, and you need to ask the advertising networks for refunds. It's important you take action and manually request refunds, as many ad networks are turning a blind eye to click fraud," added Vanes.

Polygraph uses [advanced click fraud detection](#) to identify fake clicks, including those where the website referrer is blank. "We make it easy to detect and prevent click fraud. We show advertisers which of their ad clicks are fraudulent - including the reason why the clicks are fraudulent, and provide a list of the criminal websites which are targeting their ads. The advertisers then simply block the criminal websites from seeing their ads, and use our data to get click fraud refunds from the ad networks. We have customers who are saving hundreds of thousands of dollars every month due to Polygraph. Our service is extremely powerful, yet simple to use," said Vanes.

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

Trey Vanes
Polygraph
+49 160 98058592
[email us here](#)

This press release can be viewed online at: https://www.einpresswire.com/article/584298635