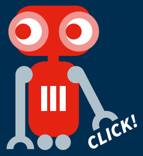
T (US) +1 917 933 2681   (UK) +44 207 802 5530   (AUS) +61 2 9096 4835
E enquiries@dianomi.com   // www.dianomi.com

dianomi™

2018

ROBOT TRAFFIC REPORT



dianomi™

DIANOMI™
ROBOT TRAFFIC REPORT

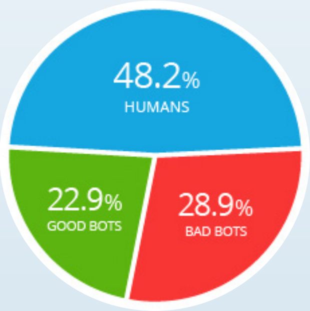
ROBOT CLICKS

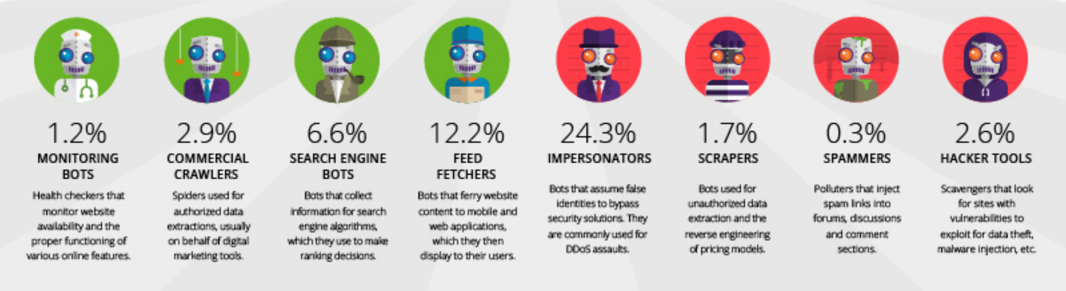
Robot clicks can sometimes account for **over 90 percent** of clicks generated in an ad campaign. While the number of robot traffic we detected in 2018 is only **32 percent**, down from **60 percent** in 2017, that figure varies greatly by month and, as recently as April 2017, was as high as **85 percent**.

Robot clicks can sometimes account for **over 90%** of clicks generated in an ad campaign.

GOOD BOTS VERSUS BAD BOTS

Although you should carefully detect robot clicks and never pay for them, **not all robots are malicious**.
The adorable line up (below) of the different types of robots by Incapsula gives you some idea who the usual suspects are:





Health checkers that monitor website availability and the proper functioning of various online features.

Spiders used for authorized data extractions, usually on behalf of digital marketing tools.

Bots that collect information for search engine algorithms, which they use to make ranking decisions.

Bots that ferry website content to mobile and web applications, which they then display to their users.

Bots that assume false identities to bypass security solutions. They are commonly used for DDoS assaults.

Bots used for unauthorized data extraction and the reverse engineering of pricing models.

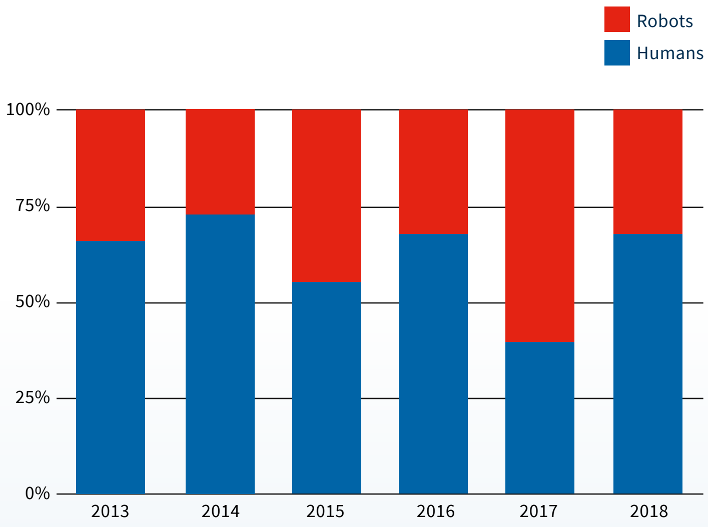
Polluters that inject spam links into forums, discussions and comment sections.

Scavengers that look for sites with vulnerabilities to exploit for data theft, malware injection, etc.

THE PERCENTAGE BOT TRAFFIC ANALYZED

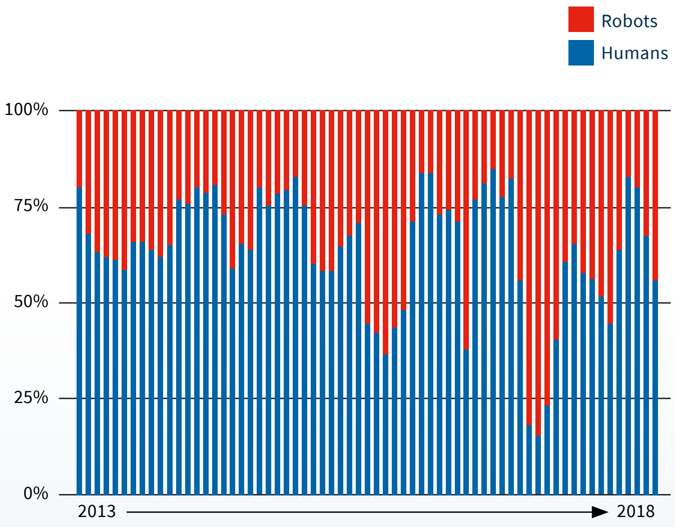
As mentioned above, bot traffic varies greatly over time and by publishers. We take a closer look below:

Since 2013, Robots have averaged **38 percent** of clicks, but **years** vary significantly from **27 percent to 60 percent**.



YEARS (2013-2018)

Months vary even more with robots responsible for **15 percent to 85 percent** of clicks.



MONTHS (2013-2018)

ROBOT CLICKS BY PUBLISHER

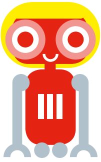
From 2013 to 2018 robot clicks by publisher varied from **2 percent to 100 percent** and that is after disqualifying any publishers generating less than 10,000 clicks over the time period.

Note that there seemed to be **little correlation between the size of the publisher in terms of the amount of clicks delivered and the percent of robot clicks.** The same is true when we look only at publishers delivering over 100,000 clicks during the period.

EMERGING TRENDS

As the ANA observed in their report entitled, Bot Baseline 2016–2017, Fraud in Digital Advertising: ***“Behind every big bot problem, someone is paying a traffic source. We observed 3.6 times as much fraud coming from sourced than non-sourced traffic.”*** This could mean that some publishers are buying traffic from questionable sources and consequently delivering more robot clicks. Bots are also getting better at resembling humans. According to ANA, **75 percent** of the fraud observed in the 2016-17 study came from computers containing both a human and a bot on the same machine.

Our data also found that some robots are becoming more sophisticated in looking like a human by, for example, having a User-Agent which is usually used by a browser, supporting javascript and spreading the clicks over a longer time frame and over several IP addresses.



Some robots are becoming **more sophisticated in looking like a human** by, for example, having a User-Agent which is usually used by a browser, supporting javascript and spreading the clicks over a longer time frame and over several IP addresses.

KEY TAKEAWAYS FOR ADVERTISERS

1. When buying clicks from a publisher or other source, you must carefully measure the amount of robot traffic that may have been delivered. Like measuring ad viewability of display advertising, measuring the number of robot clicks is critical to achieving ROI on your ad spend.

2. To make sure that you are not paying for robot clicks, you need to understand that there are standard ways of robots identifying themselves and to tell robots where they should and should not click (“robots.txt”). Crawlers from the major search engines will follow these rules and therefore don’t present a problem. Robots that don’t obey these rules, like bad robots, can still usually be identified because they behave in a way that is evidently not human.

3. We suggest employing a combination of **four** different strategies to combat click fraud and eliminate traffic coming from robots:

   - » Use a 3rd party platform to analyze the clicks: e.g. Neustar, DoubleVerify, IAS, MOAT etc. We use Neustar’s IP Reputation (IPR) Score service. Neustar creates “The Real User Score.” It provides a relative risk score between 1-5 and is based on analysis of combination of signals from IP GeoPoint data that are the highest indicators of fraud, and IP usage data across nine custom business segments to differentiate real end user traffic from non-human traffic.

   - » Automatically void any clicks coming from high-risk IP addresses. (We void clicks scoring 4 and 5 on Neustar.)

   - » Ask your ad partners to provide full transparency of the clicks with time, IP address, user agent and other data, and whether they have validated or voided them.

   - » Check any IP addresses generating click and impression counts over thresholds for any hour, day or week based on monthly and daily reports.

   - » To be extra sure, you could pass the clicks through a captcha provided by Google where the user may need to authenticate if Google determines the click is at all suspicious.