ELIMINATING BOT FRAUD: A CALL TO ACTION

BOTNET OPERATORS ARE ALREADY DEFEATING SOME COUNTERMEASURES

Several tactics that agencies and ad-tech platforms may currently regard as effective in preventing bots were mostly ineffective:

- Technical measures of viewability do not ensure humanity. Since so many bot operators have upgraded their bots to fake viewability, viewable impressions actually skewed slightly higher in bot incidence than non-viewable impressions.
- Blacklists require near real-time updating and often block significant volumes of real human audience as well as bots. Fraudsters adapt quickly.
- Optimizing campaigns with even the most sophisticated engagement metrics and attribution models did not eliminate bot traffic, because bots clone real people (getting bots credited for purchases made by real people), and bots fake engagement.
- Due to the pervasiveness of traffic sourcing, buying strictly from premium publishers did not eliminate bot traffic.

Cui Bono: Who Benefits?

Bot impressions distort the entire market by making it look as though there are more people viewing ads than there really are. The illusion of an unlimited, diverse supply of ad inventory drives the price of real human impressions down. It puts honest players at a huge competitive disadvantage, pressuring them to source traffic, too.

The motivations and temptations of various parts of the ecosystem differ significantly:

- Botnet operators extract their payments through cash-out points, the final stop in the fraud supply chain.
- Aggregators and middlemen gain reach, ensuring they never lack inventory to sell, and a diversity of bot profiles that match any conceivable audience segment.
- Publishers inflate their apparent audience size and pocket the difference between their traffic acquisition cost and the revenue received from advertisers.

FEAR IS THE UNSPOKEN OBSTACLE

The ecosystem described in this report is complex. There are winners and losers in advertising fraud today, and the scoreboard clearly is tilted in the wrong direction.

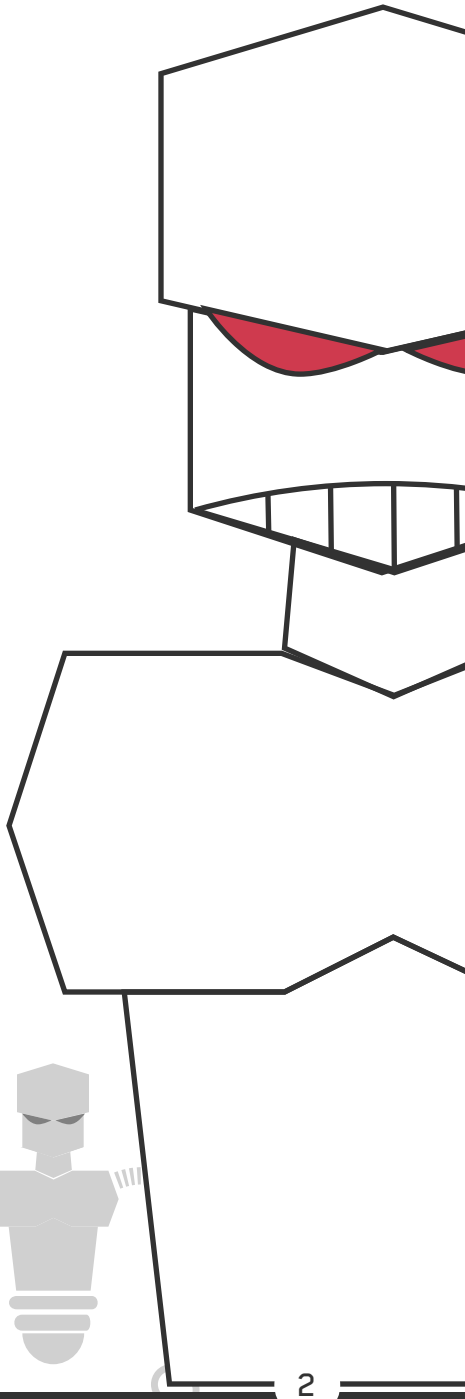
On one side, the winners are raking in billions of dollars, much of which funds cybercriminal activities by bot suppliers who have no incentive to change their behavior. Far behind in the digital advertising game are advertisers who want to offer great products to the right customers, agencies who want their media plans to reach the appropriate targets, publishers who want to support the content on their sites through pertinent advertising, and the advertising technology community who want to provide an innovative infrastructure and marketplace for online advertising.

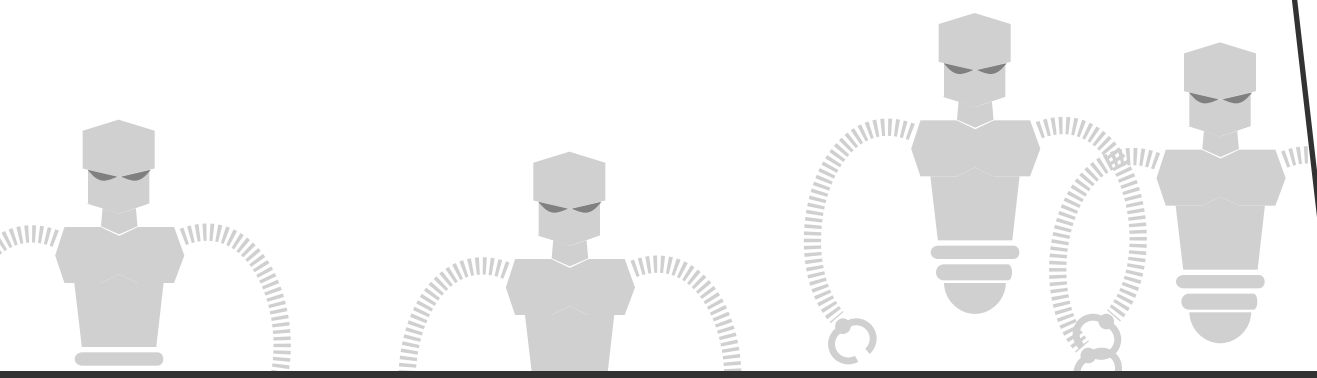
Also losing big are consumers, who are the real reason the digital ad industry exists and who have been turned into unwitting accomplices in vast networks of botnets.

The common reaction to the entire issue of fraud is fear. Fear leads to avoidance, which is just what the bad guys want. **No one wants to look unaware, unscrupulous, or negligent enough to "allow" this kind of activity to take place.**

The truth is: fraud is everywhere. No one is immune. Only by emancipating your people and partners from that fear can we get the cooperation needed to address this issue effectively.

Bot fraud is a new type of attack. Advertisers, agencies, and publishers must learn and use new concepts to understand the bot fraud threat that has emerged over the past few years. Advertisers, and all industry participants, can and must take action. Some actions can be taken unilaterally; others must be done in partnership with a fraud detection partner. The following pages provide an action plan for the stakeholders in the industry to combat fraud in digital advertising.





Action Plan for All Stakeholders

Create allies, not adversaries, in the fight against bot fraud

Bot fraud affects many suppliers in the digital advertising supply chain before it reaches the advertiser. Advertisers, agencies, and suppliers must all work cooperatively to reduce and eliminate bot fraud in the supply chain. Our call to action is for the key industry players to work both collaboratively and individually to substantially reduce bot fraud.

Manage the emotions of ad fraud discussions

Do not assume that bot fraud in your campaigns indicates an agency or publisher is deficient or bad. Remember, it's likely that your media seller is a victim of the botnet operators, not the cause.

Authorize and approve third-party traffic validation technology

This study was not deployed across all participants' placements, partly due to agency and publisher policies. Some agencies and publishers did not permit the monitoring software in certain placements (see *Appendix B: Constraints and Limitations,* page 55).

To effectively combat bots in their media buys, advertisers must be able to deploy monitoring tools. Publishers and agencies must enable the deployment of these monitoring tools. Set policy and procedures to enable advertisers to deploy bot detection and domain detection software to their ad buys.

Support the Trustworthy Accountability Group

The IAB, 4A's, and the ANA announced in early November the creation of the Trustworthy Accountability Group (TAG), a joint marketing-media industry program designed to eradicate digital advertising fraud, malware, ad-supported piracy, and other deficiencies in the digital communications supply chain. All vendors should comply with TAG's quality assurance guidelines.

While Taking Actions Against Bot Traffic, Communicate About Bots Effectively:

Within your organization, use language that accurately communicates the bot fraud problem.

Add bot-fraud discussion time to all media buy conversations internally and externally.

Adopt and use terms that correctly identify threats and real adversaries while preserving allies and building an alliance against fraud.

Action Plan for Buyers

Be aware and involved

Advertisers must be aware of digital advertising fraud and take an active and vocal position in addressing the problem. Fraud hurts everyone in the digital communications supply chain, especially advertisers. Advertisers must therefore play an active role in effecting positive change.

Request transparency for sourced traffic

Traffic sourcing correlates strongly to high bot percentages. It's recommended that buyers request transparency from publishers around traffic sourcing and build language in RFPs and IOs that requires publishers to identify all third-party sources of traffic. Furthermore, buyers should have the option of rejecting sourced traffic and running their advertising only on a publisher's organic site traffic.

Include language on non-human traffic in terms and conditions

Consider adding specific language to your terms and conditions to address the issues discussed in this study. An illustration of one approach to the definition of fraudulent traffic and the safeguards that might be negotiated between advertisers and media companies is provided in the appendix (developed by Reed Smith, ANA's outside legal counsel). You should consult with your own counsel to develop specific provisions that best serve your company's individual interests (see *Appendix D: Illustrative Terms and Conditions*, page 57).

Use third-party monitoring

Monitor all traffic with a consistent tool. Comparability is essential. Selective monitoring, such as once a month, once a quarter, or only on certain channels, encourages evasive maneuvers by bot suppliers. Third-party monitoring can validate or disprove assumptions about the quality of a publisher or ad tech company's traffic. We recommend relentless monitoring to get the best value out of your ad investment.

Use monitoring and bot detection to reveal the bots in retargeting campaigns and audience metrics. This will prevent the purchase of additional media targeted at those bots and will improve campaign metrics.

Action Plan for Buyers (Continued)

Apply day-parting when you can

Bot fraud represents a higher proportion of traffic between midnight and 7 a.m. Buyers can reduce bots by concentrating advertising during audience waking hours.

Update blacklists frequently and narrowly

Be careful how you block. For blacklists to be effective, they need to be updated at least daily, must be very specific (micro-blacklisting), and must accompany other defenses.

Control for ad injection

Ad injection (the unauthorized placing of ads on sites where they do not belong) is a tactic that causes programmatic buys to contain higher levels of fraud. Discuss with your DSP or tech platform how to control ad injection.

Consider reducing buys for older browsers

There are more bots claiming to be IE6 (2001 original release date) or IE7 (2007 original release date) than there are real humans still using those browsers. Consider reducing older browser impressions in buys.

Announce your anti-fraud policy to all external partners

In combination with covert, continuous monitoring practices, the watchdog effect will change behavior, reduce fraud, and encourage others to join the fight.

Budget for security

Across many industries, the typical cost of security amounts to an overhead of 1 to 3 percent. In the credit card ecosystem, that security spending has lowered the losses due to fraud to just $0.08 cents per hundred dollars. Lowering bot fraud in advertising to those levels could potentially return many multiples of the security spending needed to achieve it.

Action Plan for Publishers

Continuously monitor sourced traffic

Always monitor sourced traffic. Know your sources and maintain transparency about traffic sourcing. Eliminate sources of traffic that are shown to have high bot percentages. Monitor all vendors, all the time.

Protect yourself from content theft and ad injection

Use a service such as domain detection or bot detection to monitor for content-scraping (presenting another site's content in a separate website and monetizing the scraped content with ads) and evidence of ad injection. A bot detection service can measure actual numbers of bots in high-bot traffic, allowing payment for the human audience while eliminating bots from the billing process.

Consider allowing third-party traffic assessment tools

Publishers can enable advertisers to improve the granularity of their traffic performance by authorizing third-party monitoring (for characteristics such as viewability, engagement, and bot detection) and third-party tracker measurement.