VIDEOLOGY AND WHITE OPS

ERADICATING BOT FRAUD:

THE PATH TO ZERO-TOLERANCE

videology | whiteops

TABLE OF CONTENTS

INTRODUCTION

THE PROBLEM OF AD FRAUD–SPECIFICALLY NON-HUMAN TRAFFIC COMMONLY REFERRED TO IN THE ADVERTISING INDUSTRY AS "BOT TRAFFIC"–IS A HUGE AND GROWING CONCERN IN THE WORLD OF DIGITAL MARKETING. IT IS A PROBLEM AFFECTING ALL STAKEHOLDERS WITHIN THE ADVERTISING ECOSYSTEM–ADVERTISERS, THEIR AGENCIES, AND MEDIA COMPANIES.

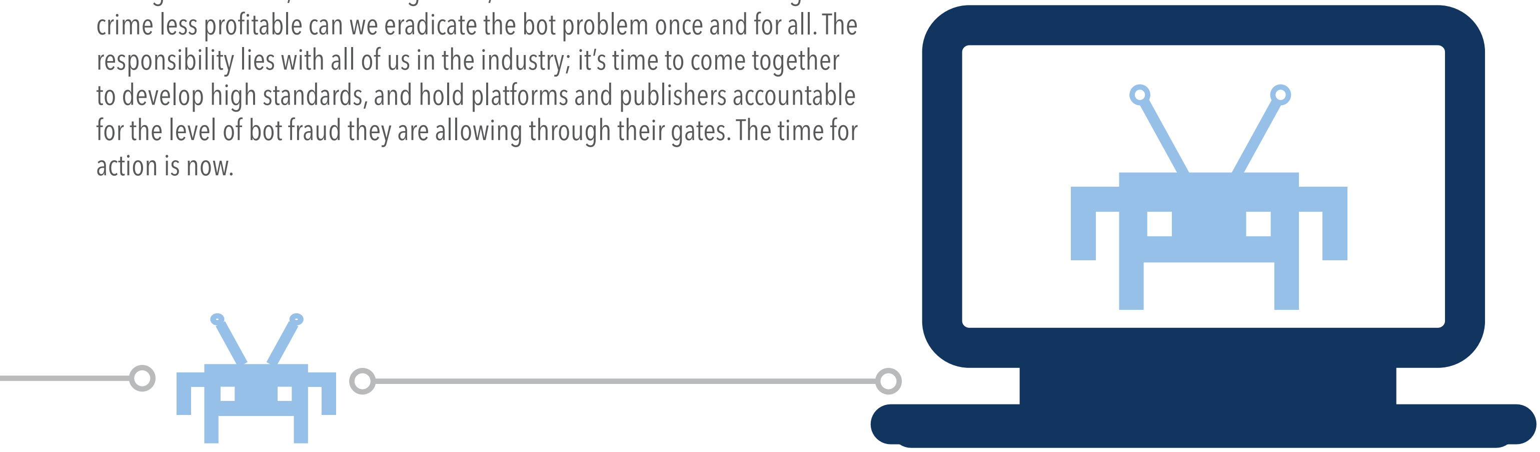
Yet, confusion still exists around the extent and nature of the bot problem in digital advertising, particularly in digital video, one of the fastest growing digital formats with the highest propensity for bots. And perhaps even more importantly, there is still uncertainty at the industry level as to what can and should be done to alleviate and eliminate the problem.

In partnership with global bot prevention leader White Ops, Videology is working to turn the tide on this growing problem by starting with education. In this whitepaper, we define the scale and underlying causes and sources of bot traffic, outline the current solutions and best-practices currently available to combat non-human traffic, and propose industry recommendations on how to proactively and definitively put bots and their perpetrators out of business. Additionally, we will share a case study that quantitatively showcases why this is all so important a study that shows how, through the right bot prevention steps, inventory can be rid of bots and drive higher brand engagement scores.

The problem is big and no one is safe; all inventory types from the low-CPM long-tail sites to the most premium and well-known publishers are infected with bots to some degree. What's important is developing solutions that don't just identify, but truly block bots and cut them off at the source. Only through education, acknowledgement, and a commitment to making this crime less profitable can we eradicate the bot problem once and for all. The responsibility lies with all of us in the industry; it's time to come together to develop high standards, and hold platforms and publishers accountable for the level of bot fraud they are allowing through their gates. The time for action is now.

"**NON-HUMAN** TRAFFIC IS AN EVOLVING ISSUE AND FRAUDSTERS WILL CONTINUE TO TRY TO FIND NEW WAYS TO AVOID DETECTION. **NHT** PREVENTION REQUIRES EVERYONE – SUPPLIERS, ADVERTISERS AND TECH PARTNERS – TO WORK TOGETHER SO WE CAN **ERADICATE BOT** TRAFFIC."

- JANA EISENSTEIN, MANAGING DIRECTOR, VIDEOLOGY EMEA



DEFINING THE PROBLEM

WHAT IS AD FRAUD?

In today's digital advertising industry, the term "advertising fraud" covers a range of deceptive practices employed by entities trying to make money using malicious techniques. Some examples include:

- AD STACKING: Piling multiple ads on top of each other, where only the top ad will be viewable, but demand side clients are charged for all ads in the stack. The ads become like layers of wallpaper–one has no idea that the wallpaper in the bathroom has 8 more layers of wallpaper underneath.
- AD INJECTION: Showing an ad on a website without the publisher's knowledge. This negatively impacts the user experience on the website, and the publisher is not compensated at all for the impressions seen by visitors.
- DOMAIN SPOOFING: When a fraudulent publisher passes a fake URL in the ad request, thereby "lying" about where the ad will actually run. For example, the ad will actually run on theavidfarmer.com, but the referring URL passed was cnn.com
- CLICK FARMS: Groups of people, often in 3rd world countries, typically paid very little money to navigate websites and mimic normal human behavior. This is sometimes done to artificially inflate traffic/site reach; otherwise, it is done to build up fake user profile/cookie data in order to make their associated bots more appealing to advertisers.
- BOTS (NON-HUMAN TRAFFIC): A malicious program or software application that runs automated tasks over the internet to simulate human activity and is financially motivated. Bots are perpetrated through the use of malware, which is a piece of software put onto a user's computer without their knowledge. Once infected, a computer will surf the web, browse on sites, click on ads, and more–all while the owner of the computer is completely unaware.

The most pervasive form of ad fraud today is the last, the use of bots, or non-human traffic. Bot fraud is often categorised along with other forms of brand safety like Viewability, which refers to the metric that tracks the level at which impressions can actually be seen by a viewer. However, while there is still dissent in the industry about the specific definition of Viewability, and how those standards should be tied to payment, there is no middle-ground with bot fraud; an ad is either being seen by a bot or by a human.

While the definition of a bot is clear, the bigger challenge is identifying and, more importantly, preventing bots to ensure a pound spent on a view is a pound spent on a human view.

WHY DOES BOT FRAUD EXIST?

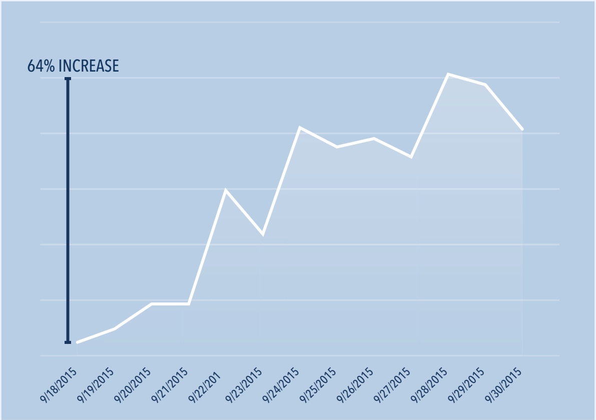
Like other forms of fraud, for example in the banking and government security sectors, fraud exists in order to make the perpetrators money. In an ecosystem like digital advertising, where so much money is changing hands so frequently, there is plenty of opportunity to take advantage of the system and hide out in the noise. This is especially true during periods when advertisers are looking for extra traffic, for example at the end of a month, a quarter, or the end of the year, when budgets are being expended [Chart 1.]

While other forms of brand safety like Viewability may vary depending on the definition, or may happen for innocuous reasons (i.e. differences in player technologies), there is no gray area with bot fraud. The use of bots in advertising is a venture in categorised crime. Bots are built and disseminated intentionally by criminals, who often disguise themselves as legitimate businesses or traffic sources.

The challenge in ridding the industry of bots is that, even when detected, it is difficult to eradicate them. Bots use computers belonging to regular people–in fact, 67% of bot fraud comes from malware infected computers behind residential IP addresses [Chart 2.] Botnet operators can easily shut down a server and move on to another victim if they are detected, and prosecution of these perpetrators is nearly impossible due to a lack of jurisdiction for authorities.

Chart 1 - AD REQUESTS IDENTIFIED AS BOTS

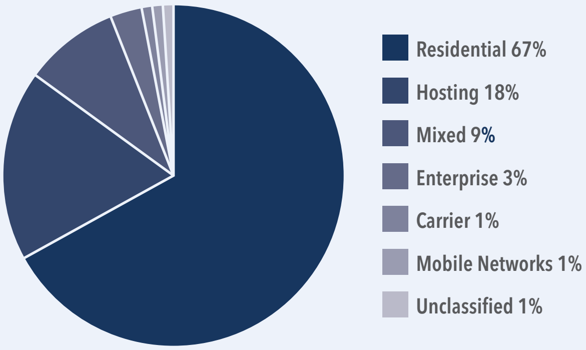
BOT TRAFFIC SPIKES DURING KEY SPENDING PERIODS, SUCH AS THE END OF THE MONTH



Source: Videology Platform Analysis, 01.09.15 - 30.09.15

Chart 2 - BOT SOURCE BY IP TYPE

THE VAST MAJORITY OF BOT TRAFFIC COMES FROM HOME COMPUTERS



Source: The Bot Baseline: Fraud in Digital Advertising; White Ops & the ANA, Dec 2014

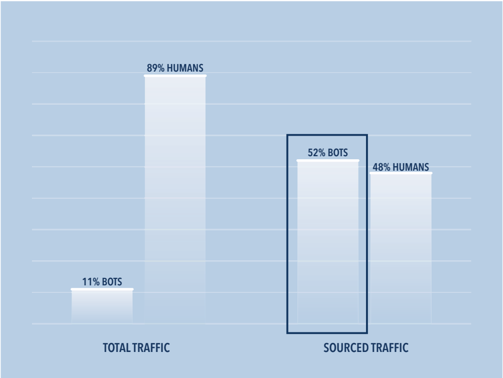
WHERE DOES BOT TRAFFIC EXIST?

Bot fraud exists across every advertising media type and across all inventory types. And while ad fraud is not a problem unique to video, video is a common target of botnets due to the comparatively high CPMs, which help make the criminals money more quickly than in display. As a result, advertisers are starting to discover that even major brands and major publishers are not safe.

There is a misconception in the industry that bot fraud only exists in long-tail, lower-priced inventory. This is not the case. Advertisers are quickly learning that premium inventory is not a safeguard against fraud. In fact, over half of bot fraud comes from 3rd party aggregators or "sourced traffic"*, who, in some cases, target premium inventory even more than longtail inventory due to the higher CPMs [Chart 3.]

Sourced traffic is inorganic traffic bought by a publisher to drive traffic to its own webpages. While the practice of purchasing the 3rd party traffic itself is typically innocent, third party traffic is often heavy with bots. Sometimes the aggregators themselves are responsible, and sometimes they are sourcing from 4th or 5th parties, which is where the problem originates. Irrespective of its origin, bot traffic disguises itself as human, and "views" ads. The publishers themselves are often unaware of any foul play, and, under pressure to hit revenue targets and deliver eCPM growth, continue to turn to these 3rd party aggregators. However, the result can be a market with artificially low pricing due to fraud–even at the highest quality level.

CHART 3 - SOURCED TRAFFIC AVERAGED 52% BOTS



Source: The Bot Baseline: Fraud in Digital Advertising; White Ops & the ANA, Dec 2014

HOW BIG IS THE PROBLEM?

It is estimated that advertisers across the globe will lose $6.3 billion to bots in 2015*; if nothing is done, this could put the dollar figure over $7.3 billion in 2016, assuming a digital ad spending growth rate of 16% next year. Specific to video, it has been estimated that 8%-23% of online video ad inventory is consumed by bot impressions, making this a major issue for video advertisers.

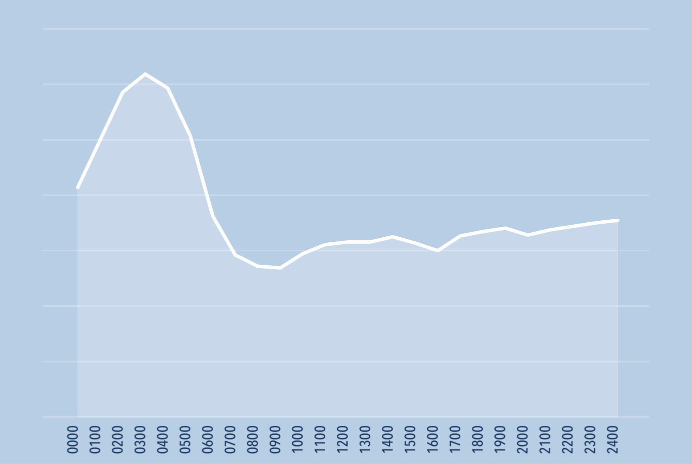
Malicious attackers are figuring out how to evade the traps set for them by stakeholders and auditors, and they are succeeding. Some placements may be well-defended against fraud traffickers while others are fully vulnerable to ad fraud theft. Stakeholders are experiencing costly fraud in inventory due to a mix of malicious adware and botnets; in fact, research shows that some campaigns can see bot levels of up to 93%*. These perpetrators are not just "skimming off the top" in a way that can be built into a CPM price; in some cases they are infiltrating entire campaigns, and creating price distortion across the advertising ecosystem.

*Source: The Bot Baseline: Fraud in Digital Advertising; White Ops & the ANA, Dec 2014

> "THIS ENTIRE INDUSTRY IN EVERY FACET HAS **UNDERESTIMATED** THE **SOPHISTICATION** OF THE **ADVERSARIES** WE'RE UP AGAINST."
>
> - MICHAEL TIFFANY, CEO, WHITE OPS

IS IT POSSIBLE TO PREDICT BOT BEHAVIOUR?

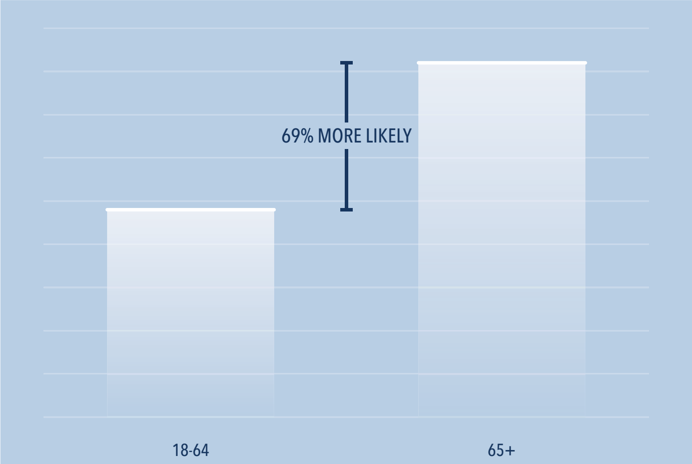
CHART 4 - BOT REQUESTS BY HOUR



Source: Videology Platform Analysis 01.09.15 - 30.09.15

A Videology/White Ops analysis of bot habits reveal some patterns for identifying bots; for example, a greater percentage of traffic contains bots during the nighttime hours [Chart 4.] This is because bots do not sleep like humans do, so while real human traffic decreases at night, bot traffic stays consistent and therefore becomes a bigger percentage of the traffic whole during those hours.

CHART 5 - BOT REQUESTS BY AGE GROUP



Source: Videology Platform Analysis, 01.09.15 - 30.09.15

Some bots focus on targeting at-risk populations, such as older age groups. In fact, those in the 65+ age group are 69% more likely to be hosting a bot [Chart 5.] This is likely due to older age groups employing outdated browsers, particularly categories of browsers which do not update automatically. Usage of an up-to-date browser can help provide baseline bot-protection for consumers; however, as explained in the next section, is by no means a cure-all for the industry-wide ad fraud problem.

While insights such as "Bots by Hour" and "Bot by Age Group" could theoretically provide some targeting guidance to bot-averse advertisers, circumventing bots is only a band-aid solution. To successfully combat fraud, cross-functional technology solutions must be in place to defeat bots before they can act.

IDENTIFYING SOLUTIONS THAT WORK

In today's digital video market, there are multiple vendors who provide bot reporting and/or prevention services at varying degrees. Some offer a broad range of brand safety services that include fraud protection, while others focus more on Viewability specifically, with the added benefit of bot protection. White Ops is an example of a company that focuses specifically on bot fraud prevention; rather than categorising broad suspicious-looking activity among other brand safety issues, White Ops solely focuses on eradicating bot fraud.

WHAT SHOULD ADVERTISERS LOOK FOR IN A SOLUTION?

Whatever type of solution an advertiser or publisher chooses to undertake, there are several elements that they should look for to ensure they are truly eliminating bot fraud at the source:

- **WHENEVER, WHEREVER:** While some ad technologies only selectively measure fraud, an always-on blocking technology ensures bots are being detected as soon as they appear, on every device, every platform, and every placement. Such a solution has the ability to prevent – not just identify – bots wherever they show up, even differentiating between human vs. bot from the same device.

- **EVERY IMPRESSION:**It's crucial that bot blocking happens at the impression level; by analysing campaigns on the impression level, rather than the URL level, advertisers would be able to "carve out" suspicious activity, rather than eliminating large swaths of media at once. For online video advertisers, who still encounter some issues with inventory scarcity, this is crucial.

- **FOCUS ON CERTAINTY:** Some traditional ad tech solutions can overestimate, underestimate or distort bot-fraud percentages in ad traffic. Only fine-grained, precise results–rather than sweeping characterisations or judgment calls–are actionable to reduce fraud. Advertisers and Publishers should ensure their solution is measuring each impression at a transaction-level, evidenced-based bot/human decision, which reveals fraud including automation and hijacking, malicious adware, and ad injection, the first time they appear.

WHY DO THESE GUIDELINES PRODUCE RESULTS?

In order to truly eradicate bot fraud, the perpetrators of these crimes need to be stopped before they can make a single pound on any campaign. The benefit of real-time, impression-level detection that blocks fraud the moment it happens, is that it closes the profit window. In comparison, services that require an ongoing learning period–even as short as 1 day–to identify a new bot infection can have no impact on the pound lost to bot fraud, because the botnets can continue to drive profit.

In the latter scenario, by the time the blocking starts, the bot has already made its money. In these cases, blocking provides advertisers with a false sense of protection, when in fact, the perpetrators are still profiting.

Making fraud unprofitable is the only way to stop it in the near future. Identifying and prosecuting the perpetrators of bot fraud is nearly impossible due to lack of jurisdiction for authorities. To end the preponderance of botnets, all sides of the ecosystem must work together to make the practice unprofitable and, therefore, force the perpetrators to move on. But as long as they can make more money, they will continue to victimise the system.

"THIS IS A GAME OF **CYBER WARFARE**. THE ONLY WAY **TO WIN** IT IS TO MAKE THE **CRIME LESS PROFITABLE**."- MICHAEL TIFFANY, CEO, WHITE OPS

DEFINING SUCCESS: CASE STUDY

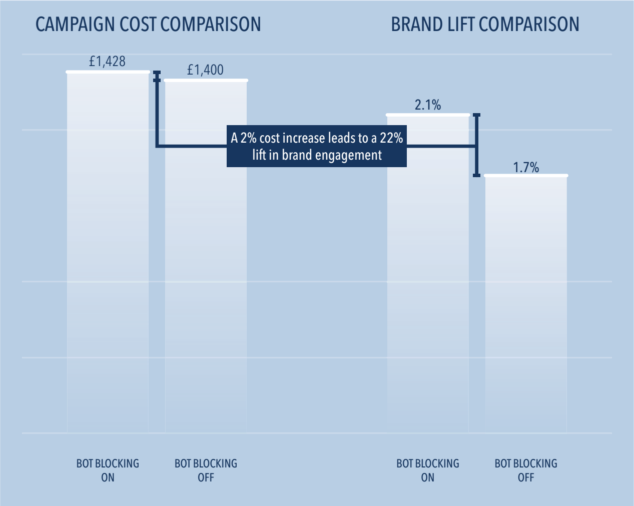
When executed properly, bot prevention can be enormously effective and cost efficient for Advertisers. To showcase the impact that the right ad-blocking solution can have on a campaign, Videology and White Ops partnered to develop a study that examines the impact of bots on brand engagement.

This analysis of the Videology platform compared brand lift-style study results on inventory with White Ops bot-blocking technology ON, versus the same video running on the same inventory, with White Ops bot-blocking technology OFF. A multiple choice survey was conducted on both media buys, with the intention of identifying brand engagement rates (determined by percentage of surveys answered) on a typical video buy versus a bot-free video buy. This approach was chosen because even the most sophisticated bots cannot fake multiple choice survey questions.

In the campaign where the client turned on bot blocking, they paid an additional £0.13 CPM. This inventory, with bots blocked, saw brand engagement rates 22% higher than the inventory without bot-blocking technology. In other words, for a price increase of only 2%, the inventory with bot-blocking technology drove brand engagement rates 22% higher on the same inventory without bot-blocking in place. [Chart 6.]

CHART 6 - BRAND LIFT COMPARISON: BOT BLOCKING ON VS. BOT BLOCKING OFF

NOMINAL COST INCREASE DRIVES DOUBLE-DIGIT IMPROVEMENT



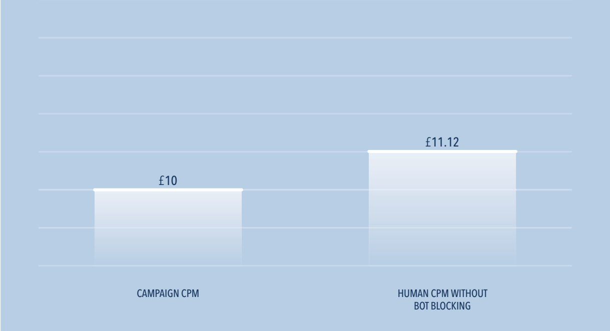
Source: 277,168 impressions on Videology Platform, September 2015

FOR A PRICE INCREASE OF ONLY 2%, THE INVENTORY WITH BOT-BLOCKING TECHNOLOGY DROVE BRAND ENGAGEMENT RATES 22% HIGHER ON THE SAME INVENTORY WITHOUT BOT-BLOCKING IN PLACE.

This analysis becomes even more interesting when considering the “Human CPM” – referring to the cost paid per human view. In this analysis, it was found that inventory not protected by bot-blocking technology had a 10.1% level of bots; therefore, if a client was paying a £10 CPM, the actual “Human CPM” for inventory not protected would in fact be £11.12 [Chart 7.]

CHART 7 - THE “HUMAN CPM”

WHEN FACTORING IN VIEWS LOST TO BOTS, THE “HUMAN CPM” BECOMES MUCH HIGHER



Source: 277,168 impressions on Videology Platform, September 2015

CAN BOTS FAKE VIEWABILITY?

According to an analysis of the Videology platform, advertisers who employ bot-blocking technology on all of their supply see baseline Viewable Rates over 9% higher than the Viewable Rate of other clients who do not employ bot-blocking. But are the bots faking it? In this case, they are not. The increased numbers were made possible by Videology’s advanced Viewability measurement solution; this MRC accredited approach employs multiple concurrent measurement methodologies, which make it difficult for even the most sophisticated bots to fake Viewability.

Source: Videology Platform Analysis, 01.09.15 - 30.09.15

> “WHEN ADVERTISERS CONSIDER THE **“HUMAN CPM”** OF A VIDEO CAMPAIGN, THEY ARE ABLE TO UNDERSTAND THE TRUE VALUE OF A **STRONG BOT-BLOCKING SOLUTION**. IT’S ALL ABOUT GETTING WHAT YOU PAY FOR.” - SCOTT FERBER, CHAIRMAN & CEO, VIDEOLOGY

WHAT ELSE IS NEEDED?

In addition to the guidelines for bot prevention that individual advertisers, agencies and media companies can follow individually or working with a bot-detection technology, there are actions that must be taken on at the industry level as well. These major shifts are the key to cutting off bots at the source and truly closing the profit window.

- DEVELOP ONE COMMON INDUSTRY STANDARD:

Paralleling the challenges that the industy experienced (and, to some degree is still struggling with) on Viewability, one of the biggest challenges the industry faces is creating a standard that all parties agree on. What, if any, level of bots is acceptable from a publisher? Who is responsible if bots do make their way into a campaign?

In today's competitive market, there are many claims from platforms and publishers about their low levels of fraud, but these claims often fall short when held up against high standards and questions of scale. In order for Advertisers to make informed decisions about how to spend their money, paradigms should be established and agreed on that follow the highest standard and the greatest intolerance for fraud. To this end, the MRC, ANA, 4As and IAB must join forces to agree on standardisation and industry-wide bot monitoring criteria so that everyone is held responsible for defeating this criminal enterprise and fairly valuing their CPMs.

- UNDERSTAND THE TRUE ECONOMICS OF COMBATTING FRAUD

  o Understand that quality, bot-free inventory comes at a cost. While the industry continues to grapple with an acceptance of the scope of the bot fraud problem, there is still a monetary advantage for publishers and ad platforms who allow bot fraud through their gates; this is a hindrance to finding a solution. It's important that the industry recognise, rather than penalise, the first movers who are fighting back against fraud, and understand that while CPMs may be a bit higher for bot-free inventory, they are paying for human views rather than bots.

  o Think in terms of the Human CPM. In digital advertising, like most other industries, there is a constant fight for the lowest CPMs. As many within the industry know, however, driving down cost is not always a good thing. It's important that as an industry, we remove the blind, procurement-driven pressure to drive down CPMs, and focus on what the real value of that view will be. The cost of 100% human views will not be dirt cheap, but will lead to humans – with money to spend – seeing ads and eventually moving down the purchase funnel to drive ROI.

  o Involve C-level corporate oversight. The conversation surrounding bot fraud should not be regarded as a simple discussion about price or about waste; it should be elevated and treated for what it is—a crime. Understanding and action around the topic of bot fraud should be happening at the highest executive levels, as it is these C-level leaders who have a fiduciary responsibility to give their clients and stakeholders what they are paying for.

WHO IS RESPONSIBLE FOR FIXING THE PROBLEM?

There is often a debate about whether fraud prevention falls to the advertiser or the publisher. The reality is, it's everyone's job: the advertiser who is making the purchase; the publisher who is providing the inventory; the platforms and technology facilitating the buying and selling.

In the end, 100% participation is key to eradicate the bot problem. The bottom line is that bot fraud is theft and everyone in the ecosystem is victimised. The problem is big and the perpetrators of the problem are getting more advanced and more sophisticated every year, so innovation must happen on the part of the industry in order to defeat them. To do so, advertisers, publishers, and ad technologies must come together with bot prevention specialists to recognise the scope of the problem and work towards a solution that cuts off fraud perpetrators before they can act.

ADVERTISERS, PUBLISHERS, AND AD TECHNOLOGIES MUST COME TOGETHER WITH BOT PREVENTION SPECIALISTS TO RECOGNISE THE SCOPE OF THE PROBLEM AND WORK TOWARDS A SOLUTION THAT CUTS OFF FRAUDSTERS BEFORE THEY CAN ACT.

ABOUT VIDEOLOGY

Videology (videologygroup.com) is a leading software provider for converged TV and video advertising. By simplifying big data, we empower marketers and media companies to make smarter advertising decisions to fully harness the value of their audience across screens. Our math and science-based technology enables our customers to manage, measure and optimize digital video and TV advertising to achieve the best results in the converging media landscape.

Videology, Inc., is a privately-held, venture-backed company, whose investors include Catalyst Investors, Comcast Ventures, NEA, Pinnacle Ventures, and Valhalla Partners. Videology is headquartered in New York, NY with key offices in Baltimore, Austin, Toronto, London, Paris, Madrid, Singapore, Sydney, Tokyo and sales teams across North America.

To learn more, contact marketing@videologygroup.com.

ABOUT WHITE OPS

White Ops is the leading provider of advanced cyber security detection and prevention services, protecting the digital advertising ecosystem and enterprise businesses against bot and malware fraud. White Ops innovative services help organizations improve their bottom lines and ensure the success of their campaigns, business goals, and the security of their systems and data. Unlike traditional approaches that employ statistical analysis, simple blacklisting or static signatures, White Ops effectively combats criminal activity by actually differentiating between robotic and human interaction within online advertising and publishing, enterprise business networks, e-commerce transactions, financial systems and more, allowing organizations to remove and prevent fraudulent traffic and activity. By working with customers to cut off sources of bad Internet traffic, White Ops makes bot and malware fraud unprofitable and unsustainable for the cyber criminals–an economic strategy that will eventually eradicate this type of fraud. White Ops was recently appointed to the board of W3C.

For additional information, contact Lexi Hughes, lexi.hughes@whiteops.com.

videology | whiteops