Radware Research

How Invalid Traffic Misclassification Causes Loss Of Opportunities For Publishers

Publishers Must Push For Transparency From Ad Verification Vendors

Table of Contents

About the Study

Overview

The one-size-fits-all solution used by ad verification vendors doesn't work for invalid traffic categorization on premium publishing sites. Many vendors do not consider domain-specific user behavior and apply a predetermined set of rules to identify invalid traffic. Traffic reports from such vendors also lack transparency about the methodologies used, and they claim that opacity is required to stop fraudsters from reverse engineering their solution.

Radware Bot Manager, we process hundreds of billions of API calls every year and protect several Alexa 500 websites, digital publishers, and ad platforms against invalid traffic. Unlike ad verification vendors, we apply challenge-response authentication and serve CAPTCHAs to visitors with high risk score to improve the accuracy of our bot detection engine. Responses to these challenges help us build a closed-loop feedback system that dynamically improves our machine-learning models, and also assist in minimizing false positives down to negligible values.

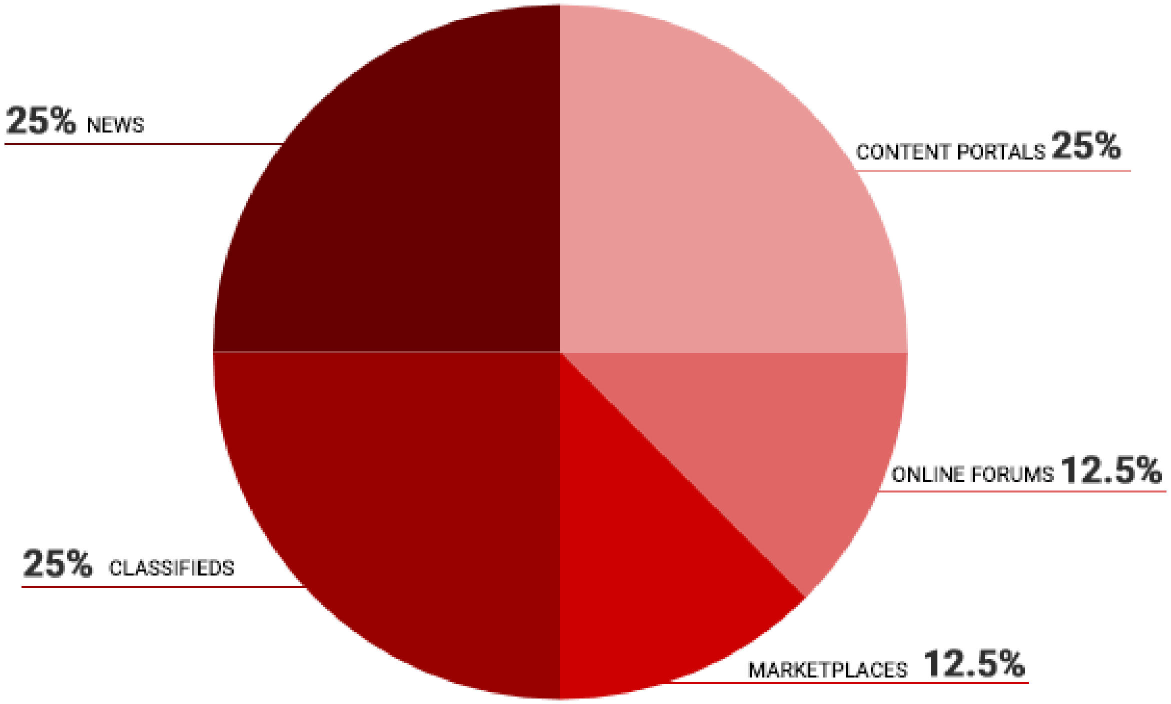
To find out why ad verification vendors erroneously categorize highly-active users as invalid traffic, we analyzed traffic reports of premium publishers by ad verification vendors. We observed that a significant number of users with distinctive usage patterns (such as browsing through IPs located in data centers, long session duration, and use of outdated browsers, etc.) are miscategorized as invalid traffic by adverification vendors.

To further understand the reasons for erroneous traffic categorization, we studied traffic sources and user engagement patterns on a premium financial publisher from the US and compared the result with that of 300 other publishing sites from different industry segments. As the financial portal's visitors comprise a vast number of business users who rely on it to make financial and business decisions, their characteristics vary from that of typical visitors of other publishing sites. The users of this financial portal can be characterized as 'power users' due to their domain-specific usage patterns — as we have
outlined in this study

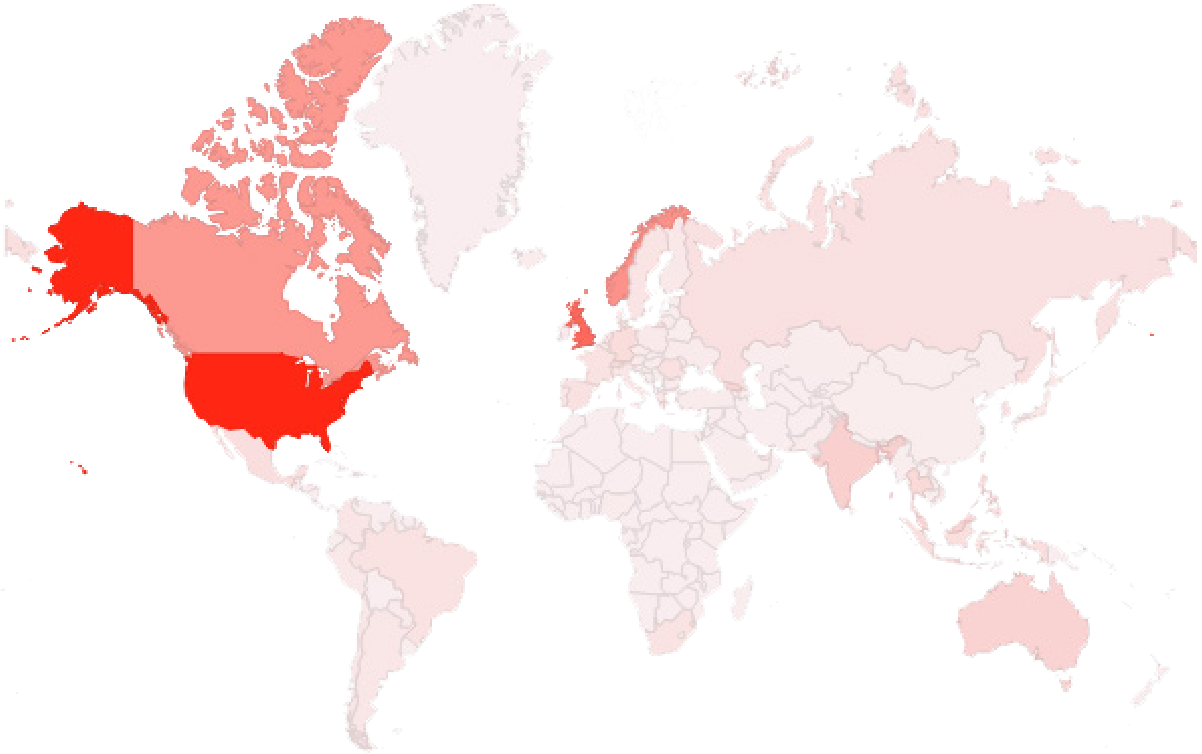
With this comparative assessment, we uncovered how users' behavior, their intent, and their organizations' Internet infrastructure could impact invalid traffic classification. We advocate more transparency in the ad verification approach and the need to have domain-specific invalid traffic detection techniques. Our results show that in the absence of a challenge-response mechanism like CAPTCHA, ad verification vendors unknowingly flag a considerable amount of human traffic as invalid

Data

For this study, we have analyzed human visitor data of a top financial portal and 300 other publishing sites over a 30-day period. The participants are from five industry segments — news, content portals, classifieds, online forums, and marketplaces



Data



Worldwide heatmap of Internet traffic considered for the study

Key Findings

- Lack of transparency in categorization and detection of invalid traffic causes loss of revenue for publishers and adversely affects the ROI on ad spend for advertisers. Invalid traffic detection solutions need to be open regarding their algorithms, approach, and classification logic to ensure that they are not causing false positives.

- Our analysis of traffic reports received from ad verification vendors unveiled that these vendors have misclassified a large number of highly-active users as invalid traffic.

- Consumers of digital publishing are of two types: highly active users of sites with live content (that is refreshed several times a day) such as the financial portal we studied, and users of media sites with relatively static content. Users on sites with live content have disproportionately higher engagement rates since they stay on such sites for extended periods to track live information including market news and stock prices.

- On average, visitors spend 7.8X more time on the financial portal compared to other publishers in a given day.

- Publishing sites that auto-refresh their content have significantly higher ad engagement rates compared to ordinary publishers.

- Visitors on average see 59 times more ad impressions on the financial portal compared to other publishers' sites.
  Ad verification vendors' generic invalid traffic detection logic based on activity-based filtration techniques is ineffective in differentiating SIVT (Sophisticated Invalid Traffic) from highly-active power users. This is why such vendors often mistakenly categorize power users as bots.

* Source - Radware Bot Intelligence 2017

- Today, many organizations use Secure Web Gateways (SWG), hosted on cloud data centers, to filter user-initiated Internet traffic. Traffic from such commercial organizations is therefore routed through data centers. Classifying all the traffic coming from data centers as invalid traffic can lead to false positives.

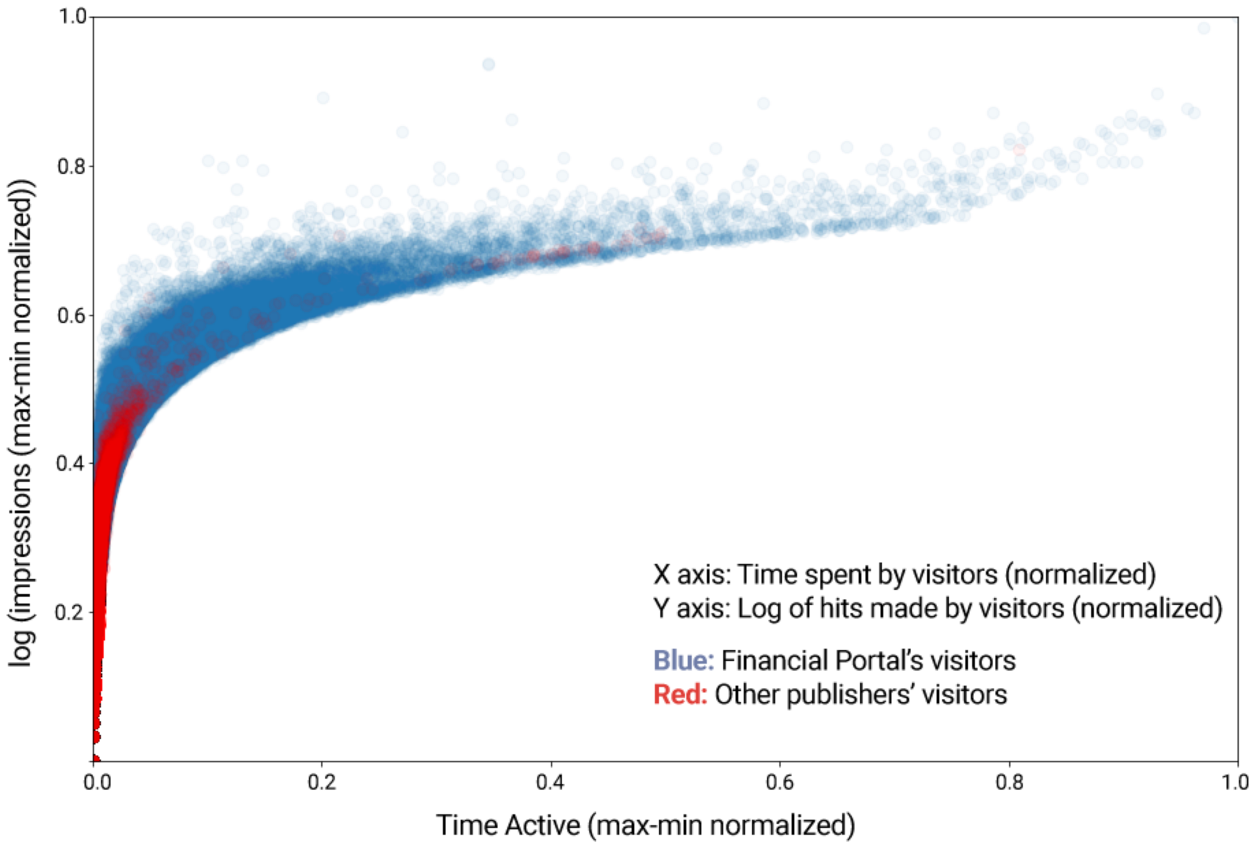
- Legitimate traffic originating from data centers is 2.9X more on the financial portal compared to other publishers' sites.

- As much as 39% of total automated traffic on publishing sites comprises SIVT.* Filtering SIVT requires dedicated bot mitigation solution to avoid false positives

*39% of total automated traffic is SIVT on publishing sites**

Power User Behavior

The financial portal offers live market data and news to users from the financial sector who rely on it to make business decisions. These users track market data and news throughout the day when stock exchanges across the globe are open. Our research reveals that on average, visitors spend 7.8 times more time on this site compared to those of other publishers in a given day.



Semilog normalized plot comparing the financial portal's visitors with other publishers' readers. The portal's users are represented by blue dots, and other publishers' readers are represented by red dots in the graph.

7.8x

On average, visitors spend 7.8X more time on the financial portal compared to other publishers in a given day.

Users spend more time on the portals with live content compared to other publishing sites.

High Ad Engagement Rate on Portals with Power Users

The site's auto-refresh feature helps power users keep track of constantly changing financial markets. Ad spaces are also refreshed independently at a higher rate than the site's automatic full-page refresh rate. Our study observes that publishing sites with an auto-refresh feature and long average session duration have substantially higher ad engagement rates compared to sites with relatively static content. Visitors on average see 59 times more ad impressions on the financial portal compared to other publishers' sites.

If invalid traffic detection techniques are not fine-tuned to consider distinctive cases of user behavior (such as the power users referred to in this study) — it can result in false positives

59x

Visitors on average are shown 59X more ad impressions on the financial portal compared to other publishers. Most of the users visits the financial portal to track live market data

Traffic from Secure Web Gateways

A relatively high proportion of users visit the portal from their workplaces. Many commercial organizations use Secure Web Gateways (SWG), hosted on cloud data centers, to filter user-initiated internet traffic. Consequently, traffic from such organizations is routed through IP addresses allocated to data centers. Our research finds that legitimate traffic originating from data centers is 2.9 times greater on the financial portal compared to other publishers' sites.

Generic invalid traffic detection logic considers all the traffic that is coming from cloud data centers as invalid traffic. Our analysis suggests that classifying all the traffic coming from data centers as invalid traffic results in false positives.

Advertisers rely on ad verification vendors' reports to plan and evaluate advertising campaigns. However, traffic reports from ad verification vendors misclassify highly-active users from commercial organizations as invalid traffic. Advertisers thus potentially miss out on opportunities to show ads to the most lucrative segment of their desired audiences

2.9x

Legitimate traffic originating from data centers is 2.9X more on the financial portal compared to other publishers' sites.

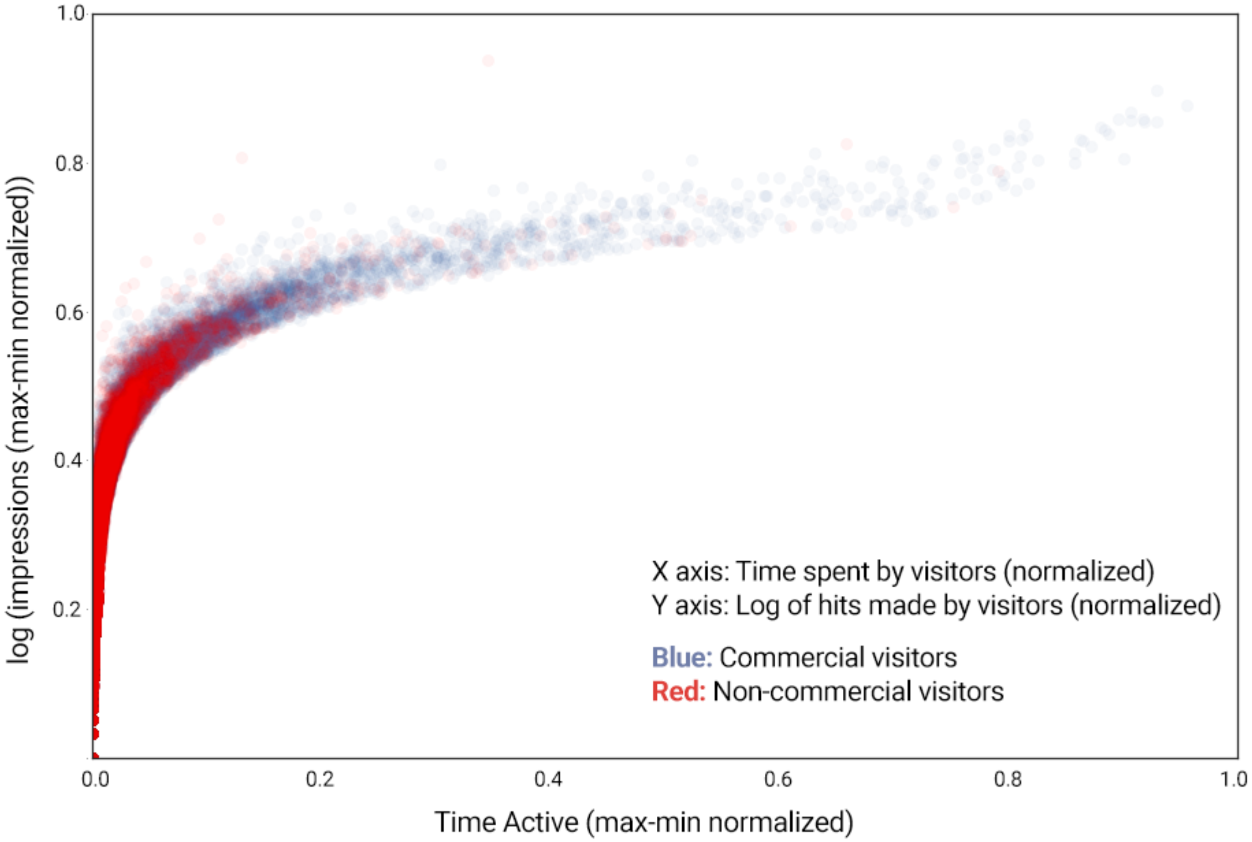
47%

*47% of internet traffic originating from data centers is legitimate**

* Source - Radware Bot Intelligence 2017

Traffic from Commercial Organizations

During the study, we noticed that a considerable number of users accessed the financial portal from their office network. These users stayed on the portal for longer periods to track constantly changing stock markets when compared to the users of other publishers that we studied. We observed that commercial traffic has certain unique characteristics compared to general traffic. These users spend 4.2 times more time and view 10.7 times more ads compared to ordinary users. Our analysis indicates that traffic originating from commercial organizations is 3.8 times greater on the financial portal compared to other publishers' sites



Semilog normalized plot comparing commercial visitors with non-commercial visitors. Commercial users are represented by blue dots, and non-commercial visitors are represented by red dots in the graph.

A significant portion of commercial visitors spend more time and generate more hits on pages compared to non-commercial visitors.

The use of outdated browsers by commercial users

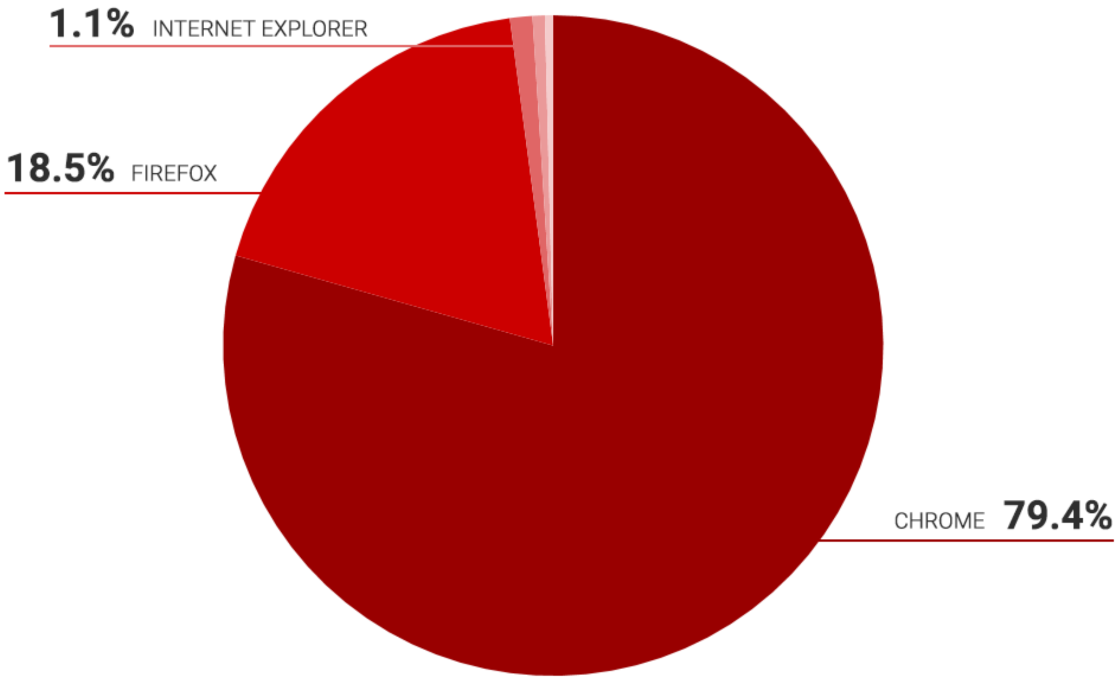
Fraudsters often use outdated browsers to create botnets and deploy bots. Interestingly, a considerable number of commercial users also use outdated browsers, as corporate policies often end up delaying browser updates. We used domain-specific machine learning models to uncover commercial users' behavior on publishing sites. Our research reveals that commercial users have a 2.2 times higher proportion of traffic from outdated browser versions compared to general users. The generic invalid traffic detection logic applied by ad verification vendors classifies the traffic based on a predefined set of patterns. Such predetermined rules categorize most of the traffic coming through outdated browsers as bots. In such cases, legitimate traffic through outdated browsers is classified as invalid

4.2x

Commercial users spend 4.2X more time and view 10.7X more ads compared to general users.

2.2x

Commercial users have a 2.2X higher proportion of outdated browser versions compared to other users.



Comparison of different types of outdated browsers used by the visitors

Auto-refreshed content

The financial portal has an auto-refresh mechanism on pages with live content. Without any manual intervention, users are shown regularly refreshed content, giving them the latest market updates and business news, as well as more opportunities to view relevant ads. In contrast, most other publishers do not have an auto-refresh mechanism as the page typically becomes irrelevant once the user reads a particular news article.

During our study, more than 2% of the portal's total impressions were made by visitors whose pages were loaded in auto-refresh mode. These users had their browser tab open with the site in focus while the auto-refresh was being executed. More importantly, we found that this portal's users have a significantly higher average session time in comparison to visitors of other publishing sites. Without paying attention to the exceptional usage patterns of such publisher's users, ad verification vendors apply generic time-series regularity detection to identify bots — such classifications categorize legitimate traffic as invalid.

2%

More than 2% of the total impressions on the financial portal were made by visitors whose pages were loaded in auto-refresh mode.

Purpose-built Bot Mitigation Solutions

The generic invalid traffic detection logic applied by ad verification vendors fails to consider exceptional behavior of power users. These vendors rely extensively on list-based common filtration procedures and fixed-parameter-based models — which are ineffective in detecting and filtering SIVT.

During our research, we observed that SIVT is relatively difficult to detect using generic methods and a bespoke solution is required to accurately identify invalid traffic, increase the transparency, and to regain the trust of advertisers. Purpose-built SIVT detection solutions that combine user intent analysis1, domain-specific behavioral modeling, multi-point corroboration, and machine learning algorithms — accompanied by human intelligence — are required to detect and filter human-like bots.

Radware Bot Manager uses proprietary Intent-based Deep Behavior Analysis (IDBA) along with device fingerprinting and collective bot intelligence to understand user intent and accurately filter non-human traffic. Unlike traditional ad verification vendors, Radware Bot Manager also applies challenge-response authentication and serves CAPTCHAs to visitors with high risk score. Responses to these challenges help us build a closed-loop feedback system that dynamically improves machine-learning models, and also assist in minimizing false positives down to negligible values.

1. Radware Bot Manager provides intent analysis to analyze the users' intent and filter invalid traffic.

Conclusion

Bots mimic genuine users' behavior to don the cloak of legitimacy and commit ad fraud. The war against ad fraud can only be won through constant monitoring, domain-specific analysis, and implementation of learnings gathered from thousands of Internet properties from relevant domains. A purpose-built bot mitigation solution that considers the distinctive behavior of users — including users from commercial organizations, data centers, and those using outdated browsers — is thus essential to accurately identify human-like bots without causing false positives.

Advertisers are concerned with non-human traffic coming to publishers' websites through paid channels. While trying to ensure a better quality of traffic, they rely on opaque reports generated by ad verification vendors that ignore domain-specific users' behavior. Such approaches cause more harm than benefit. Advertisers miss out on opportunities to target niche audiences that can be a high-value segment for them.

Ad verification vendors would also be well advised to delve deeper into domain-specific user behavior before flagging a majority of said traffic as invalid. Advertisers should insist on transparency in reports from ad verification vendors, or encourage publishers to provide traffic reports from dedicated bot mitigation vendors

About Radware

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019. ShieldSquare is now Radware Bot Manager.

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.