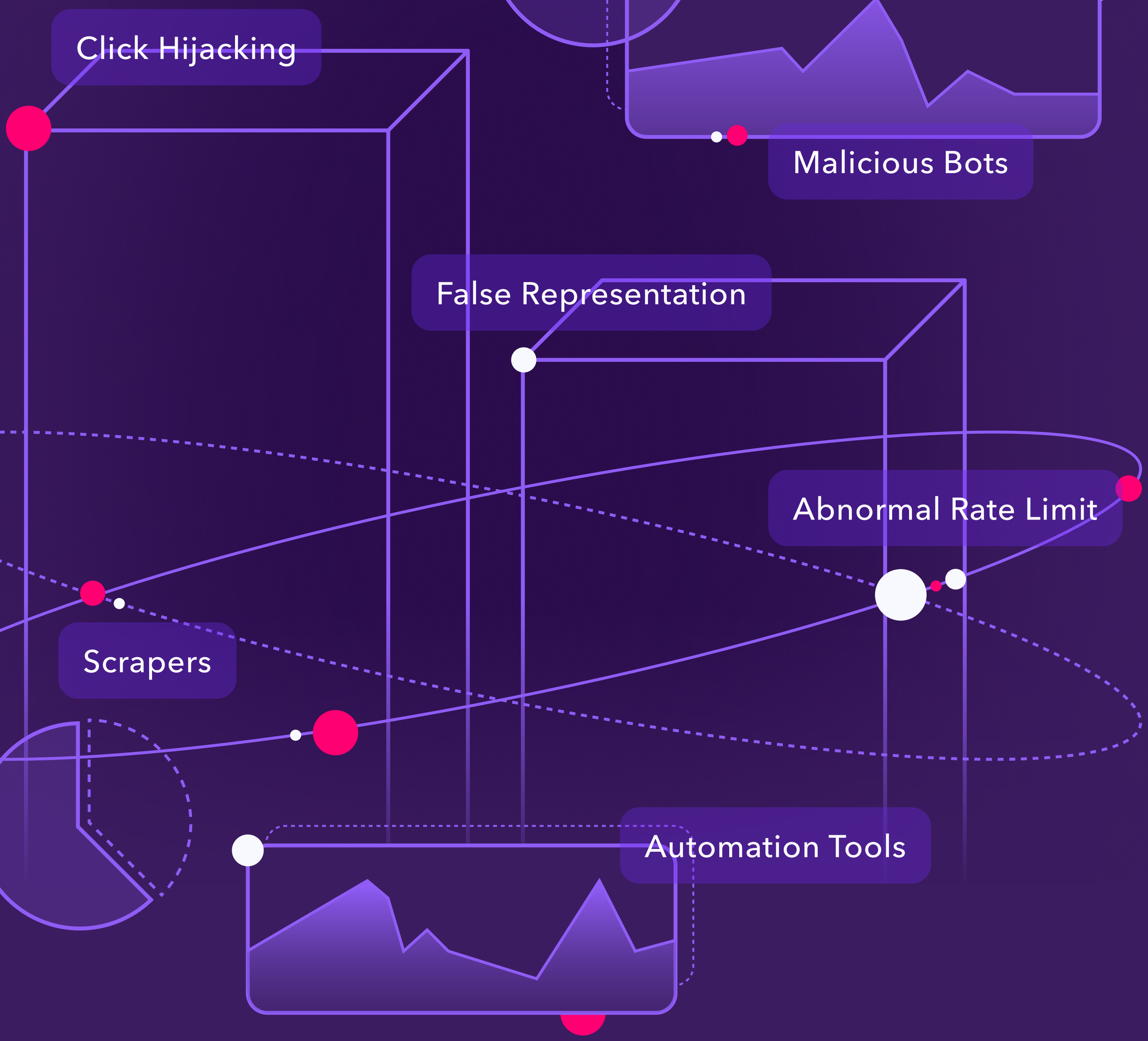
The State of Fake Traffic 2024

How bots and fake users impact business and drive inefficiency.



CHEQ

Table of contents

Introduction

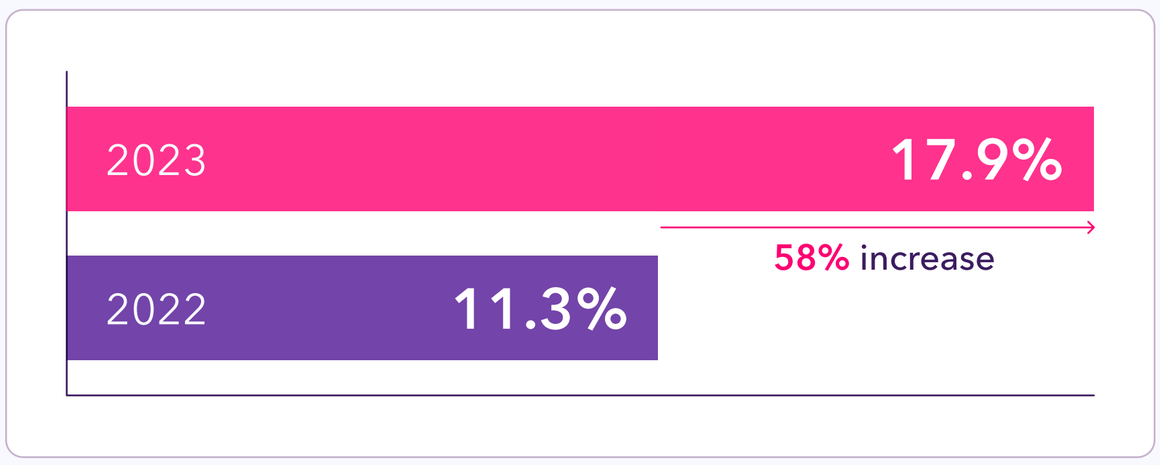
> **Imagine a world where billions of invisible hands shape the internet, manipulating online experiences and disrupting digital ecosystems, all while disguising themselves as genuine human users.**

This is not a mere exercise in imagination, it’s a stark reality. In 2024, cybercriminals and fraudsters are no longer confined to simple bots and click farms; they now wield highly sophisticated bots capable of mimicking human behavior, evading detection, and perpetrating a wide range of malicious activities. They scrape data without permission, inflate engagement metrics, commit fraud, and compromise the security and integrity of countless websites, mobile apps, and APIs.

It's a world where automation tools, both benign and malicious, share the stage with countless users who lack genuine intent.

We call this phenomenon *fake traffic*, and the problem continues to grow. In our second annual State of Fake Traffic Report, our analysis of fake traffic across thousands of domains revealed that in 2023, 17.9% of all observed traffic was automated or invalid, a 58% increase from 2022 when it was 11.3%.

17.9% of all traffic monitored in 2023 was fake.



Fake traffic isn't just a nuisance; it's a strategic business issue. Its repercussions extend from diminished advertising efficacy and distorted analytics insights to broader concerns such as operational disruptions, unauthorized data access, and the erosion of customer bases. Collectively, these issues can contribute to a decline in shareholder value, reputational damage, and even lost market share.

This year we’ve expanded our analysis to include a broader range of industries and new metrics that categorize bots by their self-reported browser, operating system, and device type, providing deeper insights into the characteristics of fake traffic.

Additionally, we examined the automation tools used to create these bots, such as Chromedriver and Puppeteer, offering a more nuanced understanding of the technologies behind fake traffic and their impact on digital environments.

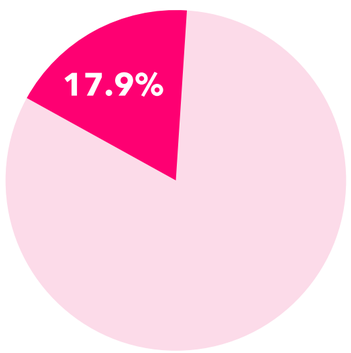
Executive Overview

The 2024 State of Fake Traffic Report offers a critical analysis of the escalating threats across the digital landscape, including automated systems, click farms, and malicious bots. The report highlights key trends, tools, and impacts on various industries.

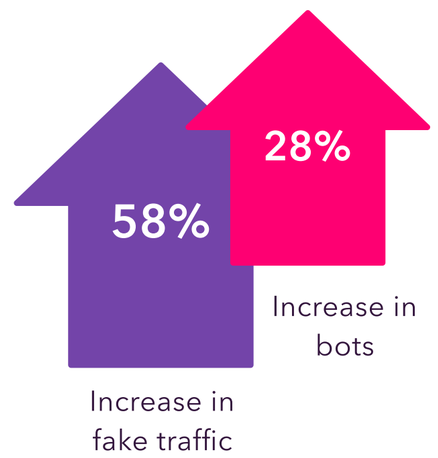
In 2023:

Bot traffic continued to grow:

- 17.9% of all traffic was fake.

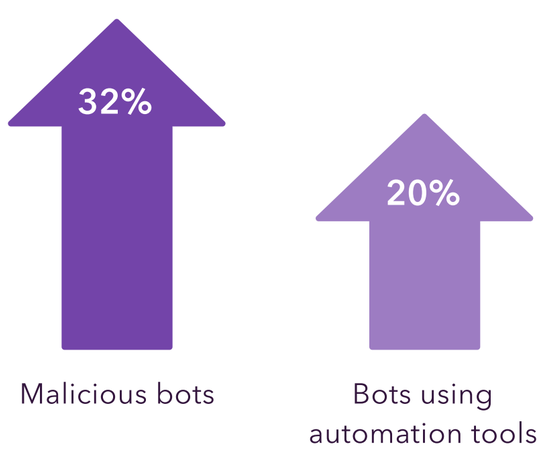


- There was a 58% increase in fake traffic overall YoY.
- There was a 28% increase in all bots YoY.



These particular threats thrived:

- Instances of malicious bots increased 32% YoY.
- Detected bots using automation tools like Selenium and Marionette increased 20% YoY.



Some industries that were highly impacted by fake traffic include:

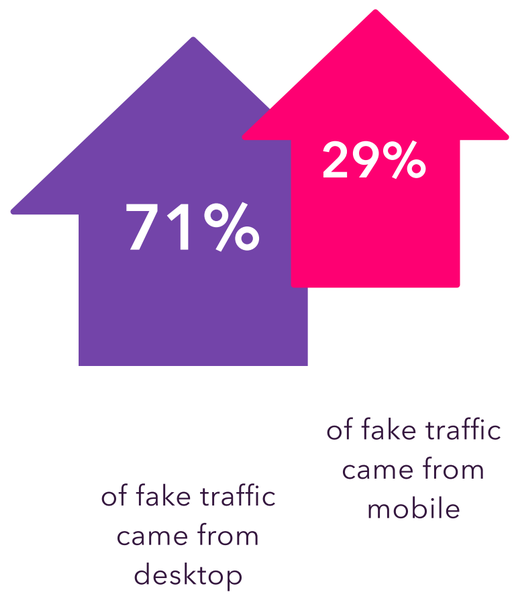
Finance
17.3% fake traffic

Retail & eComm
15.8% fake traffic

Software
14.1% invalid traffic

Bad actors preferred desktop user agents for enterprise attacks.

When looking at all fake traffic, 71% originated from desktop versus 29% from mobile.



Methodology

CHEQ evaluated each visit by conducting more than 2,000 real-time cybersecurity challenges to determine its authenticity.

The data in this report is based on a pool of 34 billion data points observed throughout 2023 from hundreds of enterprise-level CHEQ clients.

Each of these data points represents a unique interaction between a client website, application, or infrastructure device protected by CHEQ, and an array of endpoint devices, including smartphones, tablets, desktop computers, IoT devices, and embedded systems.

Whenever a device interacted with a domain protected by CHEQ, it was subjected to over 2,000 real-time cybersecurity challenges to determine the validity of the visit.

Any traffic identified as fake was immediately flagged to the client in CHEQ and integrated technologies. Traffic was categorized based on an in-depth examination of their attributes. This included investigating the sources of traffic, both genuine and self-reported, scrutinizing device types, operating systems, and browsers employed (or self-reported by the bots), as well as identifying the tools and libraries utilized in bot creation.

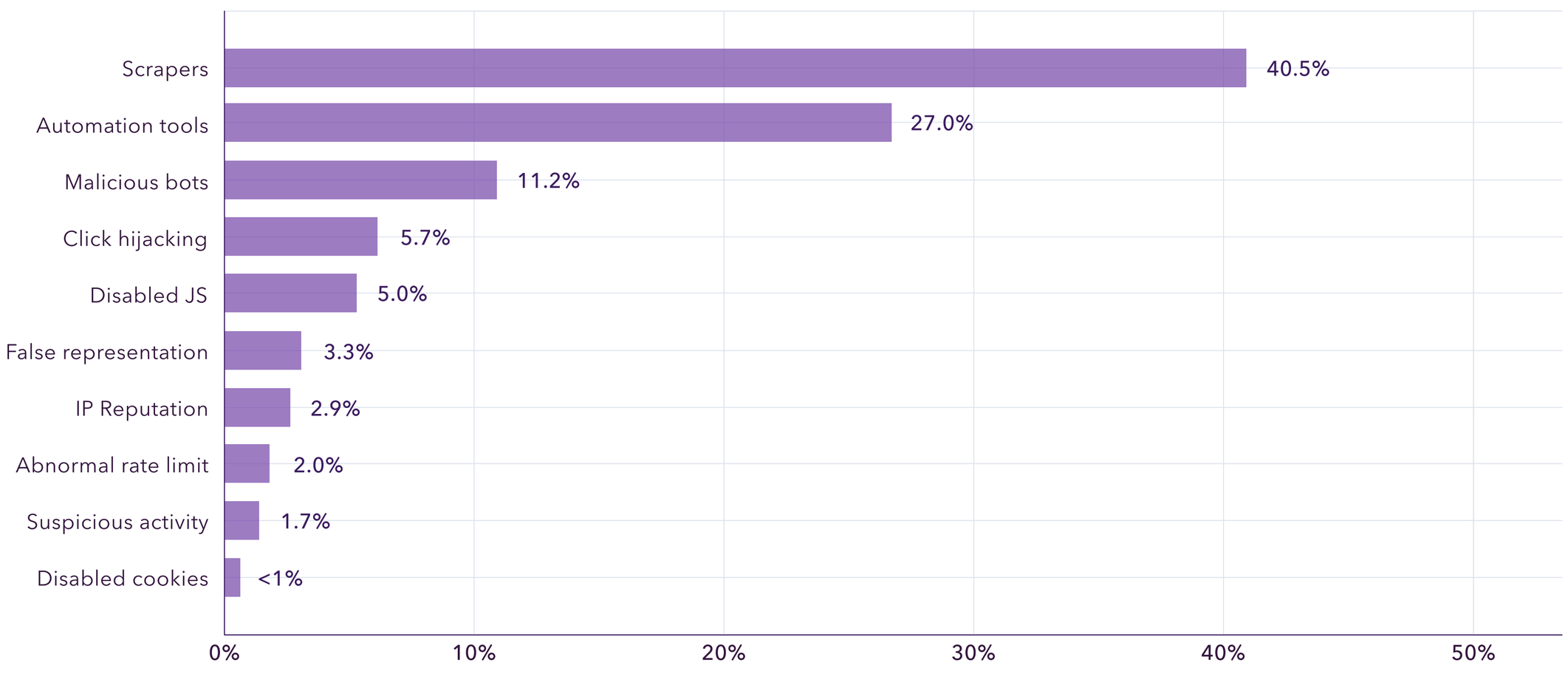
This study's overarching objective was to conduct a comprehensive analysis of fake traffic across enterprise businesses. By doing so, we furnished actionable insights and guidance concerning the characteristics, consequences, and threats posed by fake traffic.

The data presented in this report has undergone a process of normalization in which we have excluded the most extreme events to ensure that the trends represented in this report remain unaffected by uncommon or exceptional occurrences.

Fake Traffic Threat Types & Sources

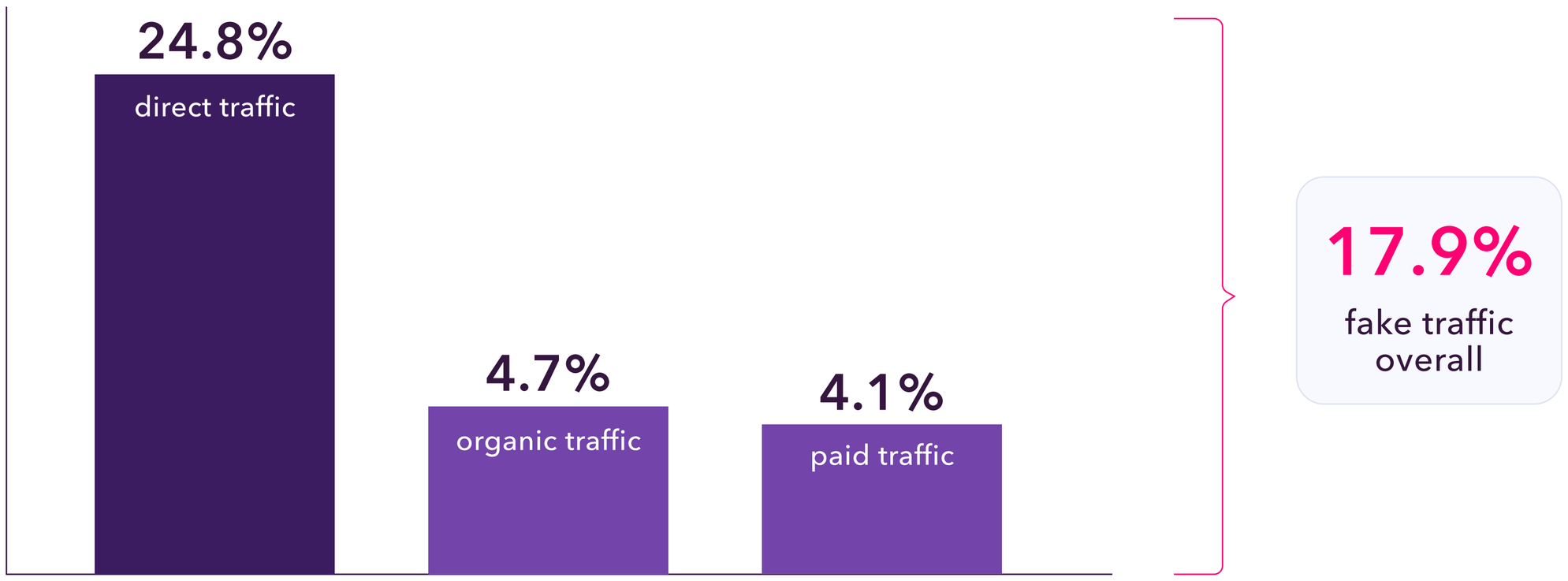
Top 10 threat types breakdown:

We analyzed the top ten threat types across all industries to find the most prominent threat types of 2023. Scrapers, automation tools, and malicious bots emerged at the top of the list. This correlates with the rise of Generative AI, which makes it easier and more accessible for users to create bots.



Fake traffic sources breakdown:

When looking at where fake traffic originates from, direct traffic saw the highest rates. 24.8% is also an increase from the 22.1% we saw the previous year. While direct traffic can sometimes show high intent from genuine users, it is also a common way for bots and bad actors to quickly access a site that that seek to attack.



Fake Traffic by Industry

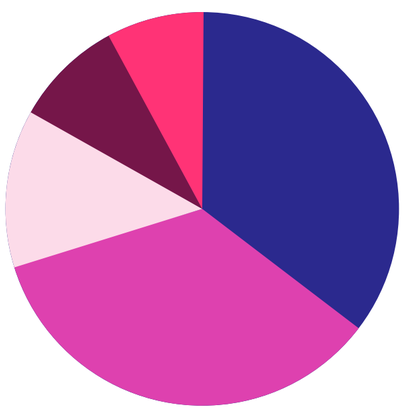
Fake traffic is a widespread issue impacting businesses of all sizes. Industries dependent on online traffic or advertising for revenue are particularly susceptible to fraudulent activity. Our data analysis from diverse clients across different regions indicates that a business's industry can greatly influence the amount of fake traffic it experiences.

A few key industries, for example Retail & eCommerce, Software, and Finance & Insurance, saw rates of 15.8%, 14.1%, and17.3% respectively.

The charts below detail the average fake traffic rate for each industry, the bot composition of the fake traffic, the five most prominent threat types, and the top sources of fake traffic.

Finance & Insurance

Financial services, banking, insurance



Breakdown of top 5 threat types:

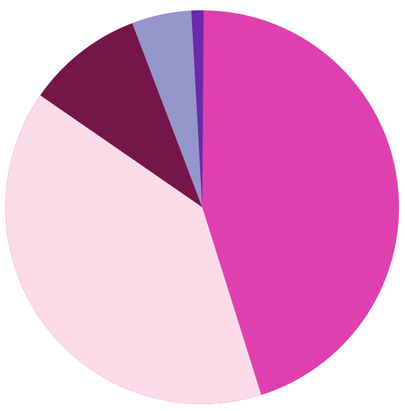
IP reputation	35.5%
Automation tools	35.0%
Scrapers	12.2%
Malicious bots	9.1%
Disabled JS	8.0%

Total fake traffic rate: 17.3%

Direct: 18.9%
Organic: 13.2%
Paid: 10.3%

Healthcare & Life Sciences

Medical services, pharmaceuticals & biotech



Breakdown of top 5 threat types:

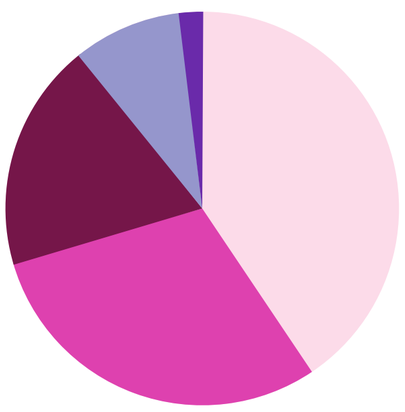
Automation tools	48.8%
Scrapers	39.7%
Malicious bots	9.0%
False representation	4.6%
Click hijacking	1.0%

Fake traffic rate: 9.5%

Direct: 17.0%
Organic: 3.4%
Paid: 2.8%

Higher Education

Nonprofit and for-profit colleges & universities



Breakdown of top 5 threat types:

Scrapers	41.4%
Automation tools	29.5%
Malicious bots	18.7%
False representation	8.9%
Abnormal rate limit	1.3%

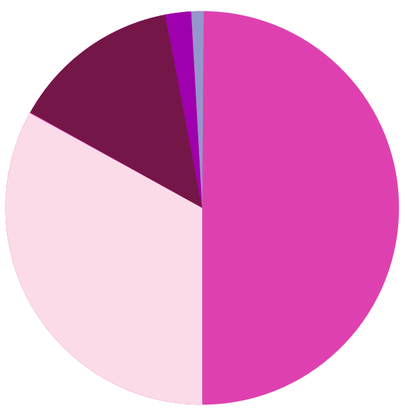
Fake traffic rate: 15.7%

Direct: 29.4%
Organic: 4.5%
Paid: 9.0%

Fake Traffic by Industry

Manufacturing

Construction, home improvement, and infrastructure



Breakdown of top 5 threat types:

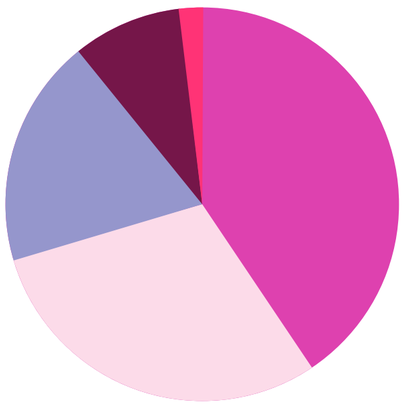
Automation tools	50.4%
Scrapers	33.7%
Malicious bots	14.0%
Disabled cookies	<1%
False representation	<1%

Fake traffic rate: 16.8%

Direct: 30.9%
Organic: 3.2%
Paid: 6.0%

Marketing & Advertising

Advertising services and marketing agencies



Breakdown of top 5 threat types:

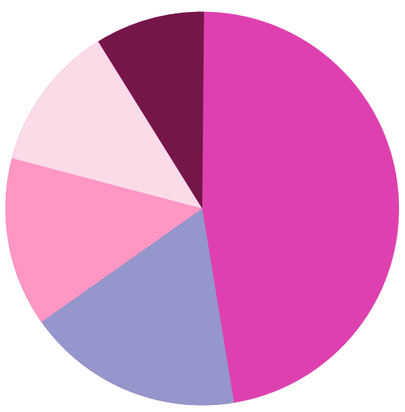
Automation tools	41.4%
Scrapers	29.5%
False representation	18.7%
Malicious bots	8.9%
Disables JS	1.3%

Fake traffic rate: 17.4%

Direct: 29.5%
Organic: 13.6%
Paid: 6.3%

Media & Publishing

Traditional and digital news publishers



Breakdown of top 5 threat types:

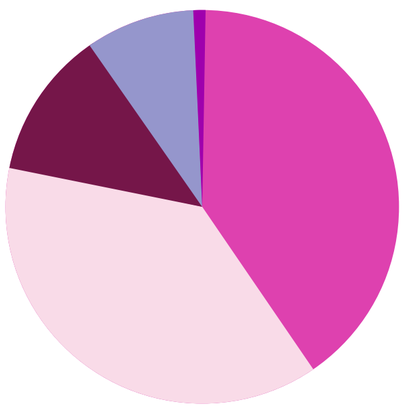
Automation tools	47.8%
False representation	17.6%
Suspicious activity	14.2%
Scrapers	11.7%
Malicious bots	8.4%

Fake traffic rate: 10.4%

Direct: 10.3%
Organic: 11.8%
Paid: 3.0%

Real Estate

Property development, leasing, and sales



Breakdown of top 5 threat types:

Automation tools	47.8%
Scrapers	37.8%
Malicious bots	12.2%
False representation	9.1%
Disabled cookies	<1%

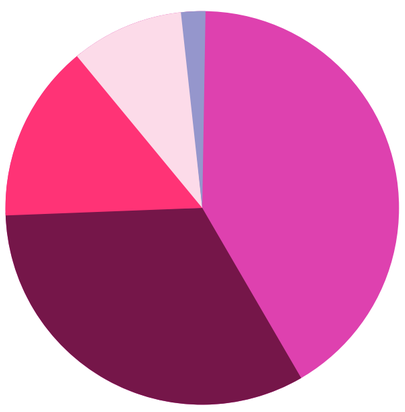
Fake traffic rate: 10.6%

Direct: 34.4%
Organic: 3.1%
Paid: 3.4%

Fake Traffic by Industry

Retail & eCommerce

Traditional, online, and direct-to-consumer retailers



Breakdown of top 5 threat types:

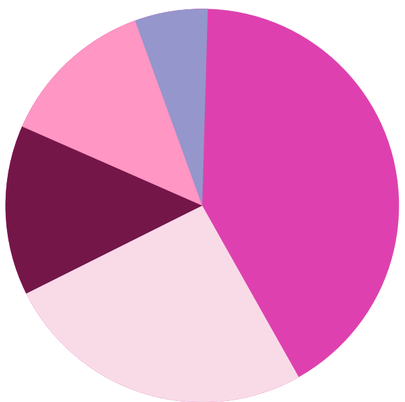
Automation tools	41.8%
Malicious bots	32.7%
Disabled JS	14.5%
Scrapers	9.0%
False representation	1.8%

Fake traffic rate: 15.8%

Direct: 32.6%
Organic: 3.75%
Paid: 3.3%

Software

Enterprise & consumer software publishers



Breakdown of top 5 threat types:

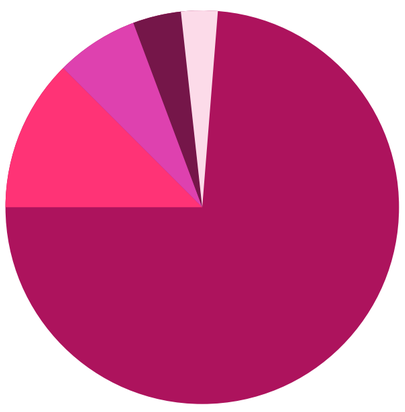
Automation tools	42.1%
Scrapers	25.8%
Malicious bots	13.5%
Suspicious activity	13.1%
False representation	5.2%

Fake traffic rate: 14.1%

Direct: 22.5%
Organic: 4.5%
Paid: 2.7%

Travel & Recreation

Travel, hospitality, entertainment companies & services



Breakdown of top 5 threat types:

Click hijacking	75.5%
Disabled JS	11.8%
Automation tools	6.1%
Malicious bots	3.7%
Scrapers	2.7%

Fake traffic rate: 11.9%

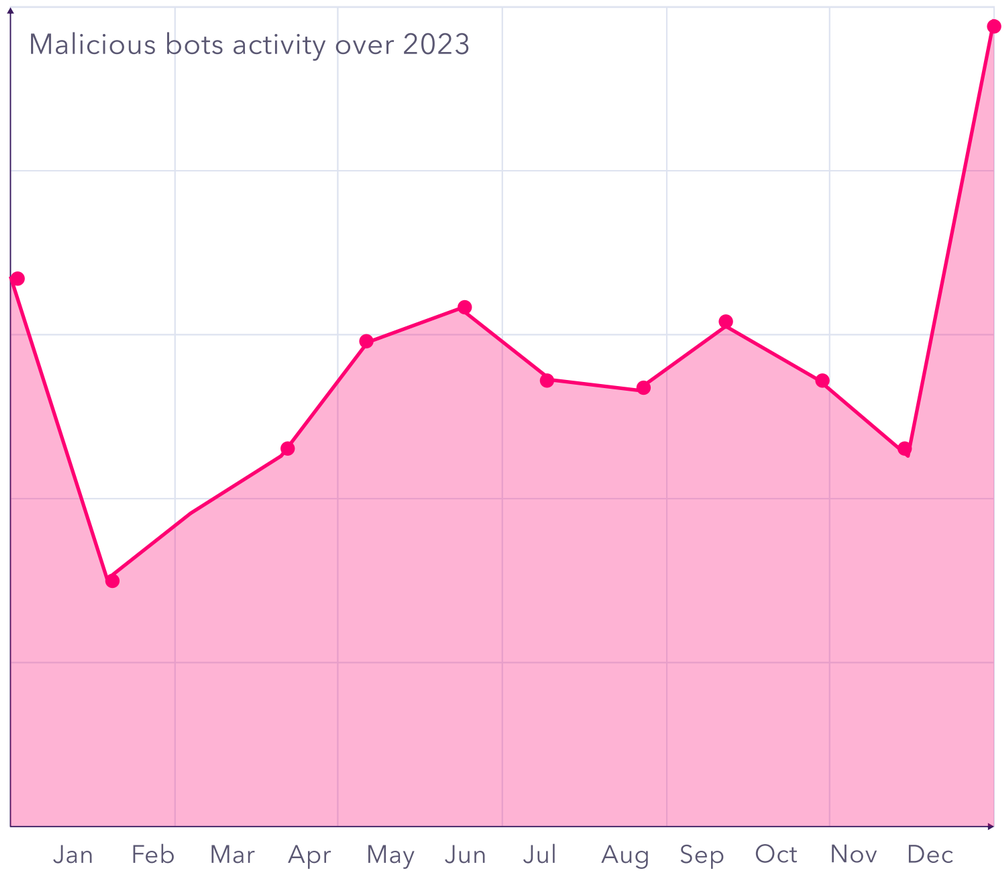
Direct: 13.4%
Organic: 3.1%
Paid: 2.4%

2023 Fake Traffic Trends: Holiday Season Surge

Malicious Activity Surged in Holiday Season

There was a significant surge in blocked malicious traffic in December 2023, predominantly driven by bots targeting the retail and travel sectors amid the holiday season.

This spike was characterized by the use of automation tools aimed at disguising the bots as human traffic, particularly in December. The capabilities of these bots posed substantial threats, from resource draining to denial-of-inventory attacks.



Case-Study: The Rise of Bots-as-a-Service

Another contributing factor to the late-year surge in malicious traffic in 2023 was the rise of Bots-as-a-Service (BaaS) platforms. These platforms offer readily available, sophisticated automation tools that can be employed by individuals with minimal technical skills. This added convenience and accessibility has broadened the scope of potential attackers, allowing for the orchestration of widespread attacks with little effort.

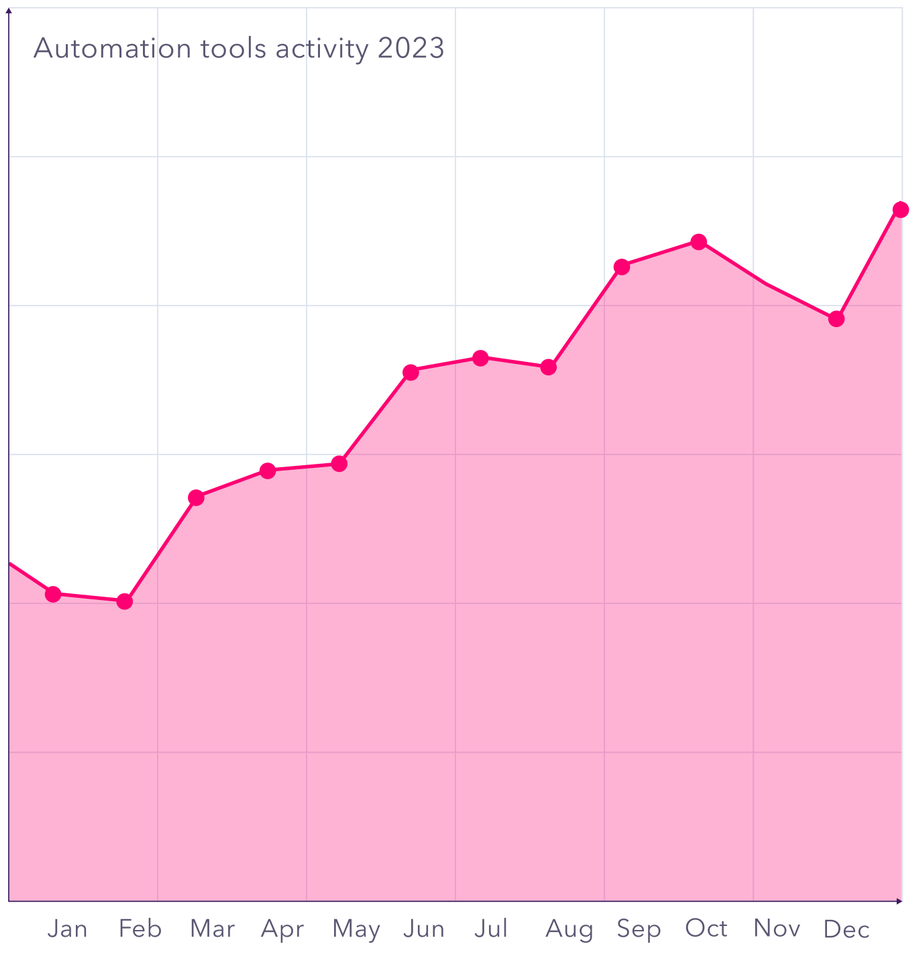
A notable case in point was a targeted attack on a travel industry domain carried out in December. We detected a well-known BaaS platform driving a 14x increase in attempted fraudulent click-throughs via Google Search Ads, seemingly a deliberate attempt to deplete the target's PPC budget during a critical sales period.

2023 Fake Traffic Trends: Automation Tools

Basic Browser Automation Tools Accounted for 24% of all Fake Traffic in 2023

In 2023, basic browser automation tools accounted for 24.0% of all fake traffic. The retail and eCommerce sectors suffered the highest incidence by volume, suggesting the widespread use of these tools for scraping and abuse.

The most frequently detected automation tools were Selenium, a popular open-source browser automation framework, and Marionette, Mozilla's automation driver for controlling and interacting with the Firefox web browser.



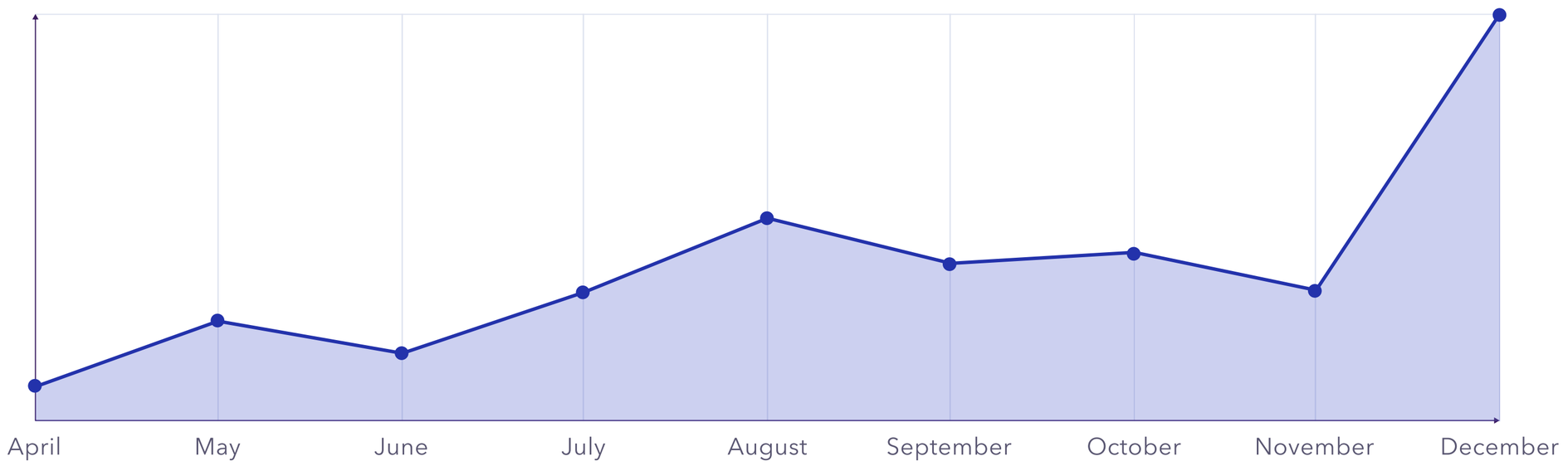
2023 Fake Traffic Trends: Advanced Evasion Techniques

Tracking Increased Use of Undetected ChromeDriver and Puppeteer-extra-plugin-stealth

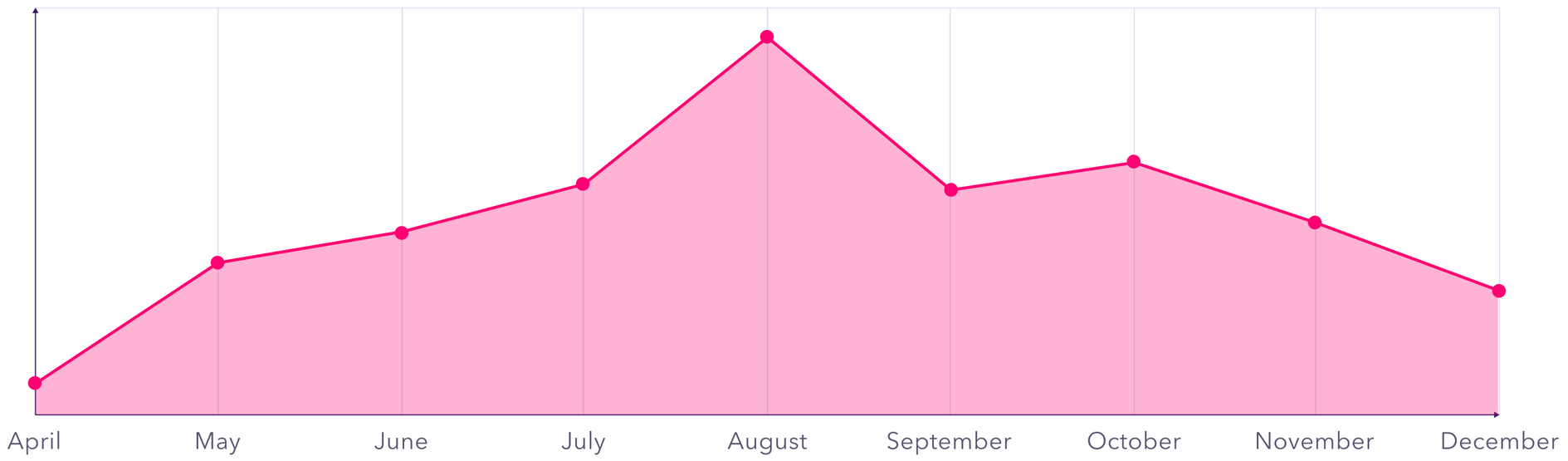
Headless Chrome has been a boon for both developers running automated tests and bot makers automating malicious web traffic. However, its use in automation can be easily detected through fingerprinting and via certain properties like “navigator.webdriver.” To counteract this, bot makers have turned to sophisticated tools like undetected ChromeDriver and Puppeteer-extra-stealth-plugin, designed to mask automation signals and mimic human interactions more closely. These tools modify browser attributes checked by anti-bot systems, making automated browsers appear as regular user browsers.

Our data underscores the rising adoption and potential impact of these evasion tools. In the second to fourth quarters of 2023, the usage of undetected ChromeDriver surged, with detected instances increasing by 650% throughout 2023. Similarly, deployments of Puppeteer-extra-plugin-stealth, the more common tool of the two, increased by 414% at its peak usage.

Bot running on undetected ChromeDriver, Q2-Q4, 2023



Puppeteer-extra-plugin-stealth, Q2-Q4, 2023



2023 Fake Traffic Trends: User Environments

Fake Traffic by User Environment

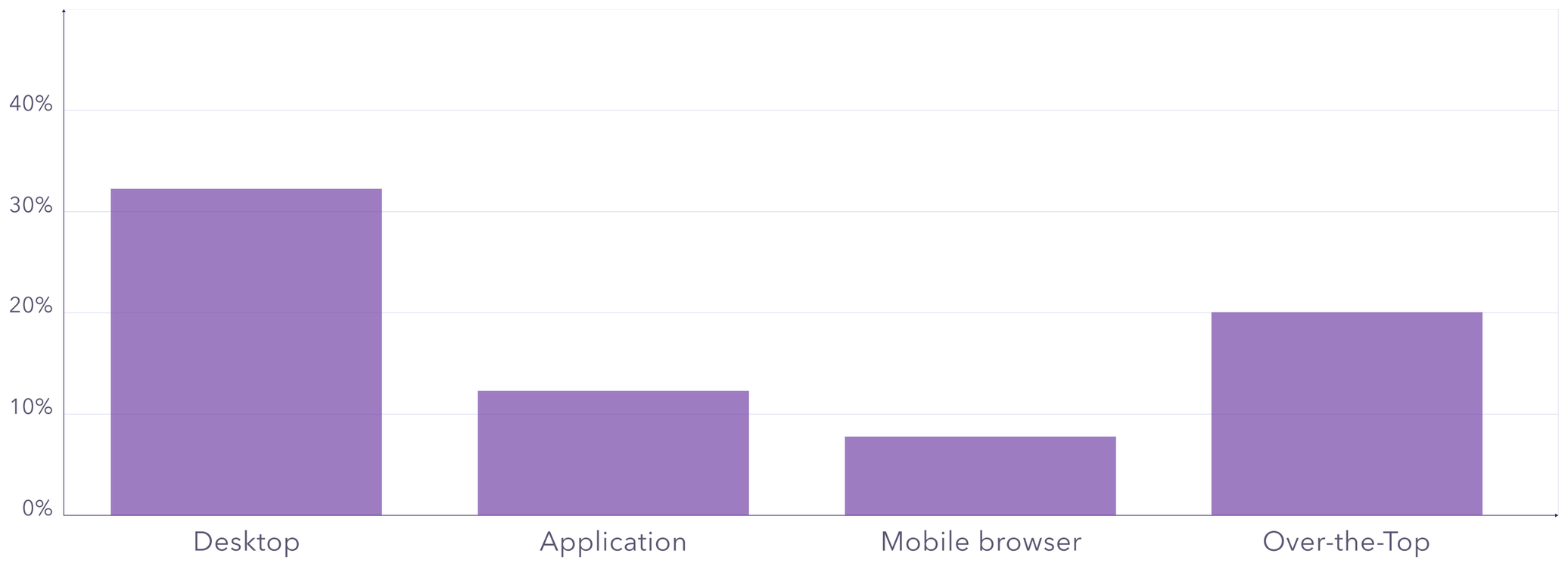
Analyzing fake traffic by the (claimed) user environment categorization reveals significant disparities, with desktop platforms experiencing a high invalid rate of 32.6%, illustrating a continued focus by attackers on these traditional computing environments, due to both familiarity and their extensive use in business and enterprise settings.

The standout 20.4% fake traffic rate for Over-the-Top (OTT) environments, technology that delivers streaming content via internet-connected devices, is driven both by the relatively high costs associated with OTT advertising ($25–$40 CPMs on average) and the nature of OTT ad delivery.

Server-side ad insertion (SSAI) allows advertisers to seamlessly insert ads into content, but it can also inadvertently open the door to ad fraud by preventing client-side ad verification tools from assessing ads' legitimacy, masking user data, and enabling ad stacking and domain spoofing.

Conversely, the mobile web shows a markedly lower invalid rate of 7.9%, reflecting less attention from attackers due to perceived lower yields compared to desktop or OTT platforms.

Fake Traffic by Environment



2023 Fake Traffic Trends: Operating Systems

Fake Traffic by Operating System

Our analysis reveals startling insights into the prevalence of fake traffic across different devices in 2023, shedding light on emerging trends among bad actors.

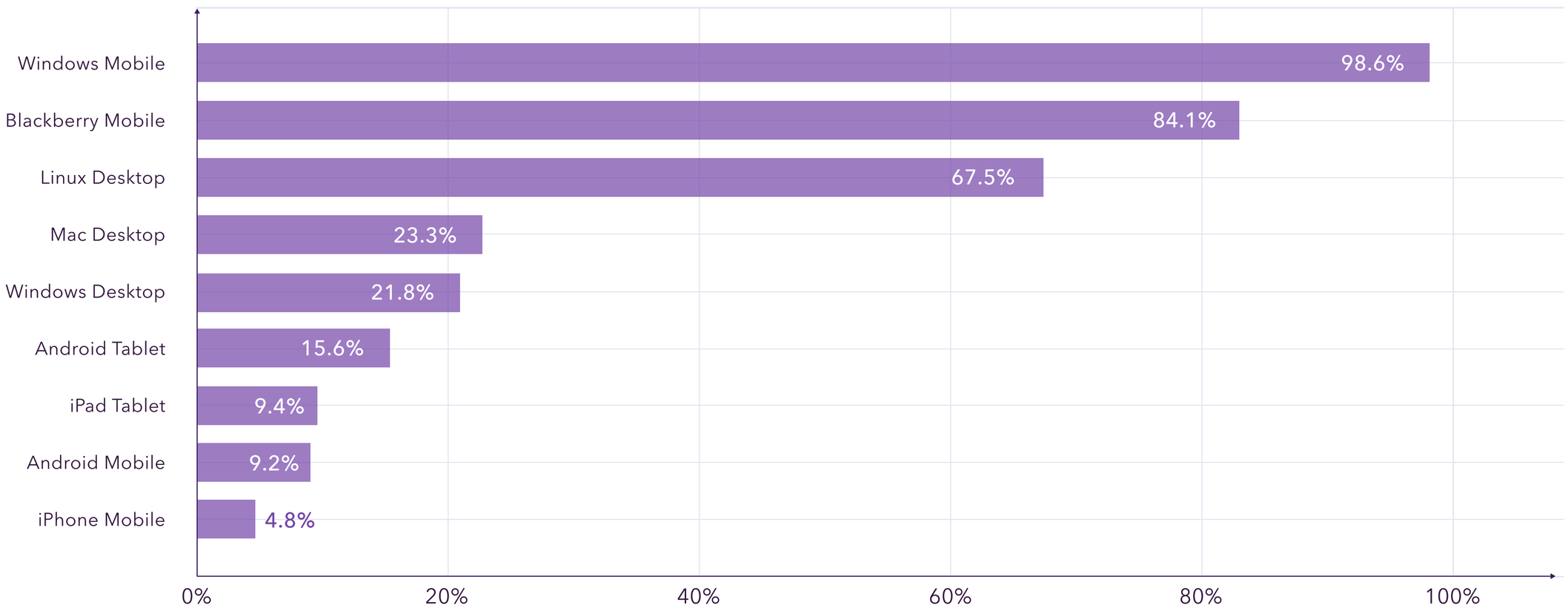
An interesting phenomenon is this: the relatively small amount of traffic observed from defunct mobile platforms–Windows Mobile and Blackberry– had by far the highest fake traffic rates of any mobile OS.

This is likely due to outdated bots, which may not have been updated for years, rather than cybercriminals raiding recycling bins for their click farms. There is also a small chance that attackers are (unsuccessfully) disguising themselves as niche platforms in an attempt to go unnoticed.

These findings emphasize the importance of scrutinizing traffic sources and implementing robust verification mechanisms to mitigate the impact of fraudulent activities.

Furthermore, the elevated fake traffic rates observed on prominent desktop devices compared to prominent mobile counterparts underscore the attractiveness of desktop platforms to fraudsters. The inherent ease of orchestrating bot attacks on desktops presents a significant challenge for marketers, as these deceptive practices skew performance metrics and erode trust in digital advertising channels.

Operating Systems by Fake Traffic Rate



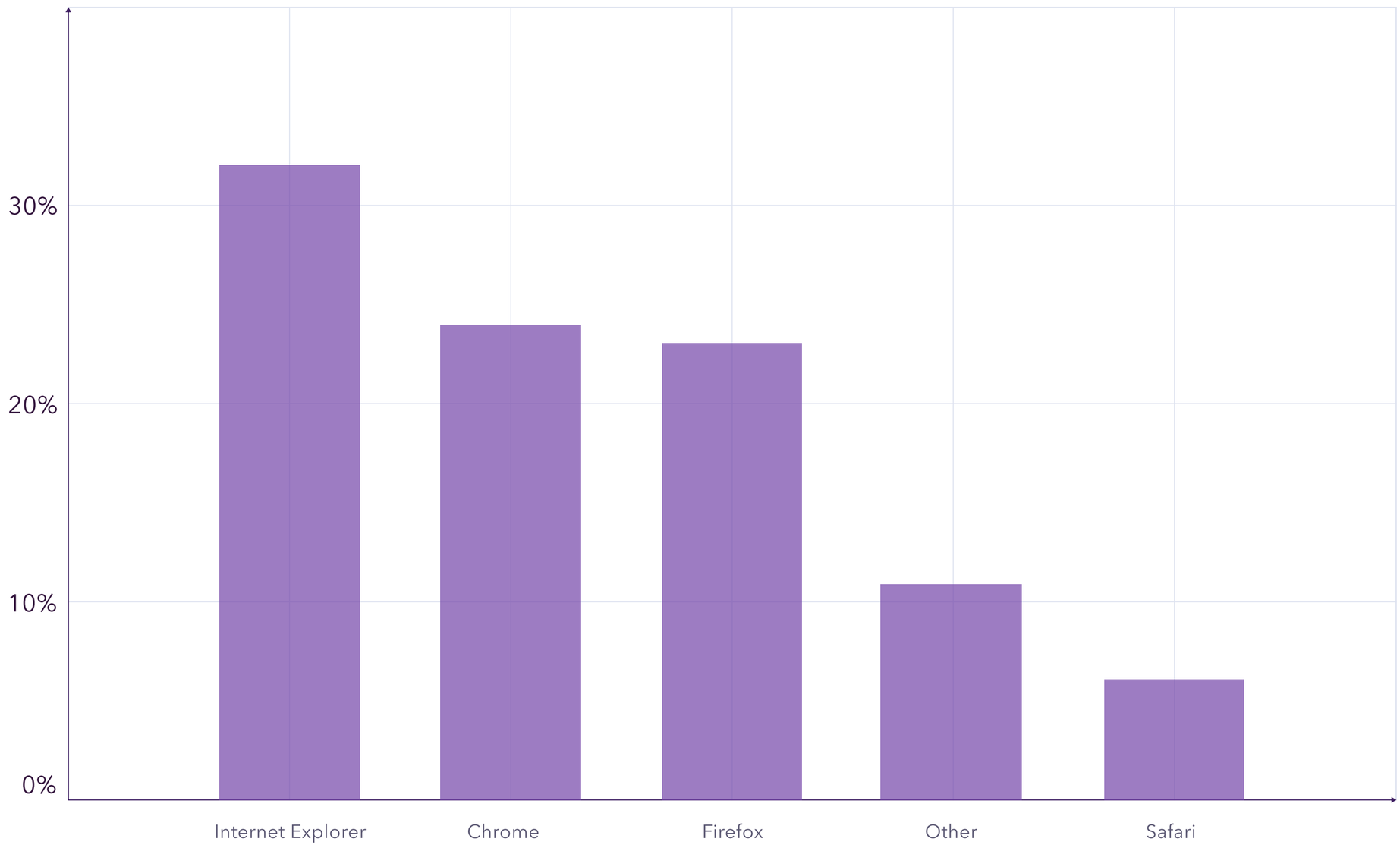
2023 Fake Traffic Trends: Browser Details

Fake Traffic by Browser

Examining browser information extracted from user agents offers another layer of insight into the dynamics of fake traffic. Namely, it highlights fake traffic's need to fit in with the crowd.

Internet Explorer (IE), despite its smaller user base, had a higher fake traffic rate of 31.9%, proving there is still a market for older or less frequently updated browsers amongst bad actors looking for a platform more susceptible to exploitation.

Browser by Fake Traffic Rate



Summary

The threat landscape posed by bots and fake traffic remains dynamic and pervasive, demanding proactive and adaptive measures from businesses across all sectors. With 2023 being the breakout year for Generative AI adoption, there is a new dimension to consider in this landscape. Generative AI technology has the potential to democratize the creation of bots, rapidly spread misinformation, and expose businesses to potential for copyright infringement via language learning models. This accessibility could lead to an influx of new bots flooding digital platforms, amplifying the risks associated with fake traffic and automated attacks.

By remaining vigilant and continuously refining defenses, businesses can mitigate the risks associated with bots and fake traffic, safeguarding their assets, reputation, and bottom line in the ever-changing landscape of cyberspace. Embracing proactive measures that account for the advancements in AI technology will be crucial in staying ahead of emerging threats and maintaining a secure digital presence.

About CHEQ

CHEQ is the global leader in Go-to-Market Security. Trusted by more than 15,000 companies, ranging from emerging brands to the Fortune 50, CHEQ protects business-critical digital interactions from malicious, automated, and human-driven threats.

Powered by its unrivaled, context-specific detection engine, CHEQ offers the most comprehensive set of solutions for securing go-to-market operations from threats to business continuity, brand reputation, privacy compliance, and marketing effectiveness. It's why CISOs trust CHEQ, marketers love CHEQ, and more businesses choose CHEQ.

See how bots and bad intent are harming your go-to-market efforts. Request a free site scan today.

Customers Love Us on G2