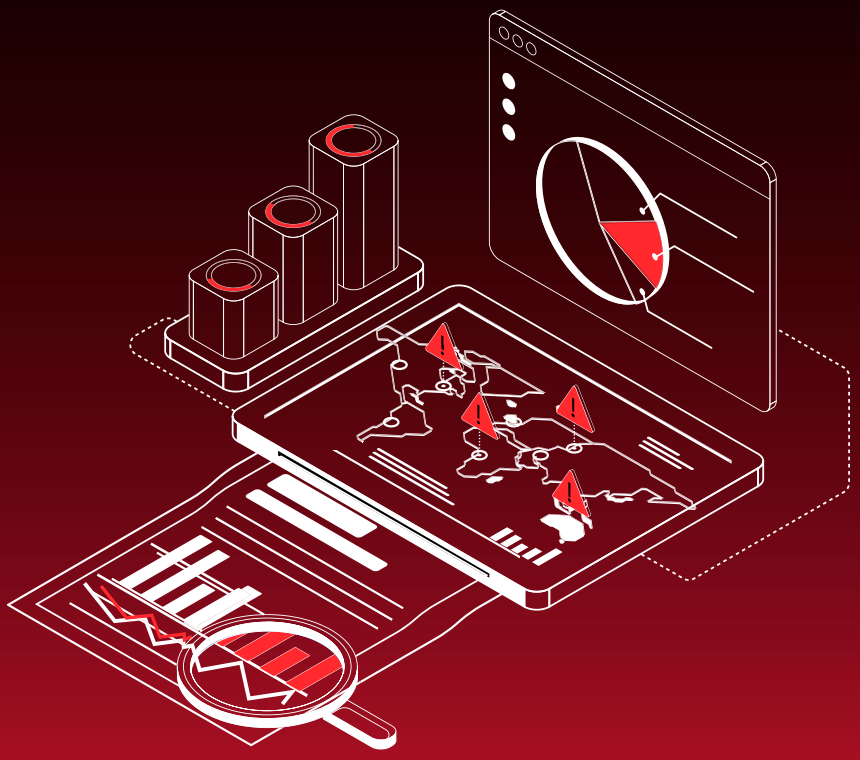
fastly

Fastly Threat Insights Report

More volume, more scrutiny – Bot trends and how organizations are responding



The Fastly Threat Insights Report highlights security trends, attack vectors, and threat activity across the application security landscape. Drawing from trillions of application and API requests across our global customer base, the report offers a real-time view into what's materially impacting security teams in the context of larger trends.

This quarter's insights are derived from traffic analyzed across Fastly's Next-Gen WAF and Bot Management products between July 1, 2025, and September 30, 2025. These solutions collectively protect over 130,000 applications and APIs* and inspect more than 6.5 trillion requests per month**. Fastly's broad visibility spanning edge and cloud-native architectures, combined with our presence across a wide range of industries, including leading e-commerce, streaming, media and entertainment, financial services, and technology organizations, provides us with a unique and comprehensive view of the global web application threat landscape.

Executive Summary

Bots have evolved beyond just a security problem, affecting teams across the business, including sales, marketing, operations, and many more. The bot conversation is now taking place within the C-Suite, as they find ways to adapt their business models to this new reality. In this edition, we'll explore emerging trends and insights that indicate how industries are addressing both wanted and unwanted bot traffic.

Key Findings

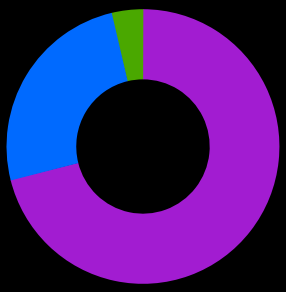
At a high level, we found that the distribution of bot traffic to human traffic appears to be similar to that in previous quarters. Deeper analysis revealed a more nuanced reality:

- **Headless bots are targeting transaction-heavy industries.** 89% of headless bot traffic targeted Financial Services and Commerce industries.
- **Organizations are blocking wanted bot traffic.** 4% of all **wanted** bots were blocked by organizations - primarily those operating in the Media & Entertainment and High Technology industries.
- **Meta and ChatGPT account for the highest proportion of AI crawler and fetcher traffic.** 60% of all AI crawler traffic is attributable to Meta, and 68% of all AI fetcher traffic is attributable to OpenAI's ChatGPT.

*130,000 App deployments protected as of 04-22-2025
**~6.5 trillion Average NGWAF Requests Inspected Monthly for the trailing 6 months as of 04-22-2025

Visual Overview

Humans vs Bots in Q3



- Humans **(71.11%)**
- Unwanted Bots **(25.33%)**
- Wanted Bots **(3.56%)**

Humans vs Bots Q/Q

Bots

2% ↑

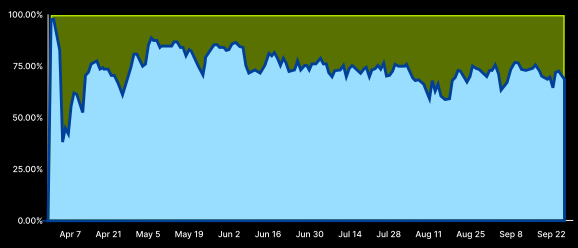
Humans

2% ↓

Wanted Bots

71% are crawlers

29% are Fetchers



60% of all AI crawler traffic is attributable to Meta.

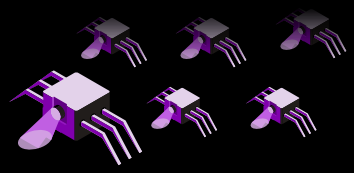
Meta

68% of all AI fetcher traffic is attributable to OpenAI's ChatGPT.

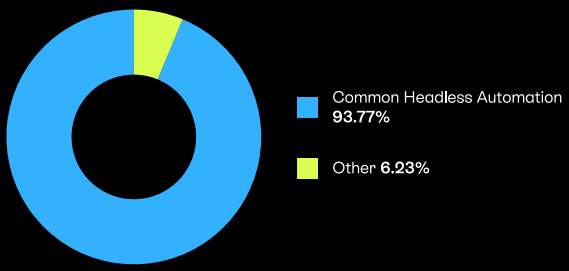
OpenAI

Unwanted Bots

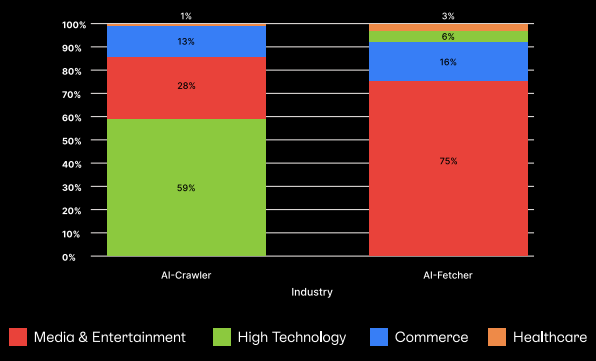
Billions of requests were from Headless bots, an emerging class of unwanted automation



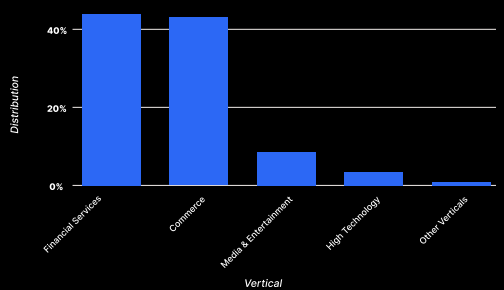
'Common Headless Automation' accounted for **94%** of total headless bot traffic



4% of wanted bots are blocked



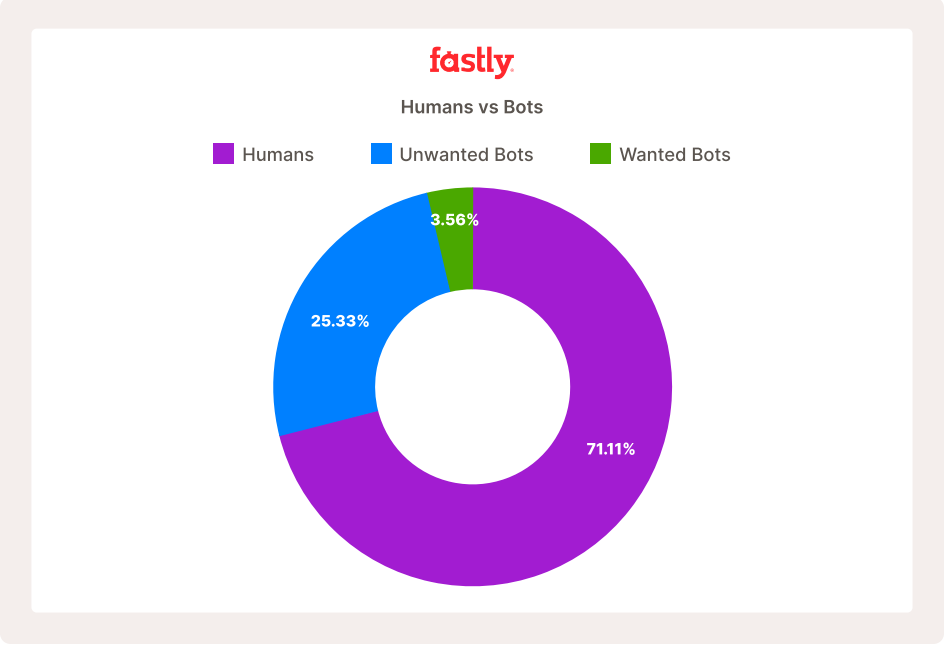
Headless bots are targeting transaction-heavy industries. **89%** of headless bot traffic targeted Financial Services and Commerce industries



Bot Landscape

The Traffic Landscape

Examining Q3 traffic across human, **unwanted** bots, and **wanted** bots activity, humans comprise the most significant portion of traffic at 71%. Bots made up 29% of all traffic, with **unwanted** bots accounting for 25%. This represents a substantial amount of traffic that can have negative implications, which we address throughout this report.

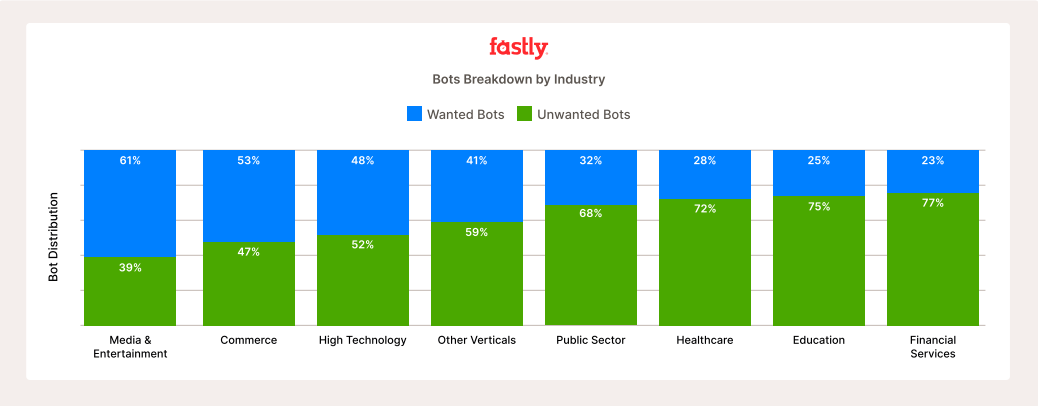


Bots by Industry

An organization's **wanted** bot policy is often influenced by the amount of traffic it sees from these three traffic sources. Examining just the distribution of Q3 **wanted** versus **unwanted** bot requests, by industry, revealed a vastly different distribution across verticals.

We saw the most **wanted** bot traffic in Media & Entertainment (61%) and Commerce (53%). This may be due to the dynamic and timely nature of these industries' content and product listings, which are highly sought after by this category of bots.

In contrast, Financial Services (77%) saw the highest distribution of **unwanted** bots, which could be an indication of desire for the sensitive data (PII, credit card information) that this industry often stores.



In this edition, we took our analysis a level deeper in order to examine a category of **unwanted** bots that target both Financial Services organizations and the other verticals we monitor: **headless bots**, which we'll address in the following section.

Unwanted Bot Trends

The Threat of Headless Bots

Headless bots are fully functional automated browsers used to mimic real user behavior on websites, but at machine speed and scale.

Historically, they've been leveraged by developers to automate tasks that don't require a graphical user interface, such as automated testing, web scraping, and monitoring. They are more efficient than traditional browsers because they run faster and use fewer resources, making them ideal for programmatic interactions with web pages.

These qualities, however, make them ideal for cybercriminals. These bots can execute JavaScript and mimic human activities, allowing them to bypass more simplistic anti-bot solutions. These bots can perform web scraping, ad fraud (e.g., simulated clicks on Google Ads), DDoS attacks, credential stuffing, and more.

While the implications of successful headless bot misuse are concerning, the real challenge for businesses is the difficulty in identifying (and blocking) unwanted activity facilitated by headless bots. Not only can they mimic legitimate users on the surface, they're often leveraged by internal development teams for completely legitimate purposes like end-to-end UI tests, or performance monitoring and synthetic testing.

1. **The duality of the problem requires organizations to not only identify this traffic type but to also understand their usage internally in order to prevent unintended consequences.**
2. **Allowing all headless traffic creates opportunities for cybercriminals to engage in nefarious activities under the guise of a legitimate user.**

Blocking all headless traffic or specific libraries without business context can lead to SDLC impacts, as developer tools are blocked from completing needed testing.

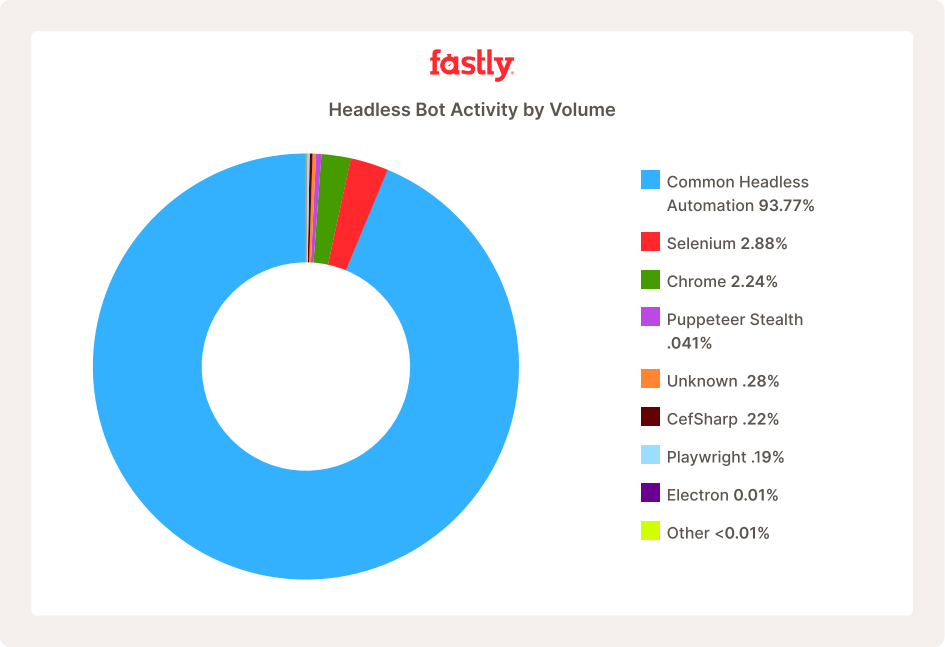
Given that this nuanced problem is unique to every organization, we examined headless bot activity to identify any broad trends that can be learned from.

Headless Bot Activity

In Q3 alone, we saw billions of requests from headless bots.

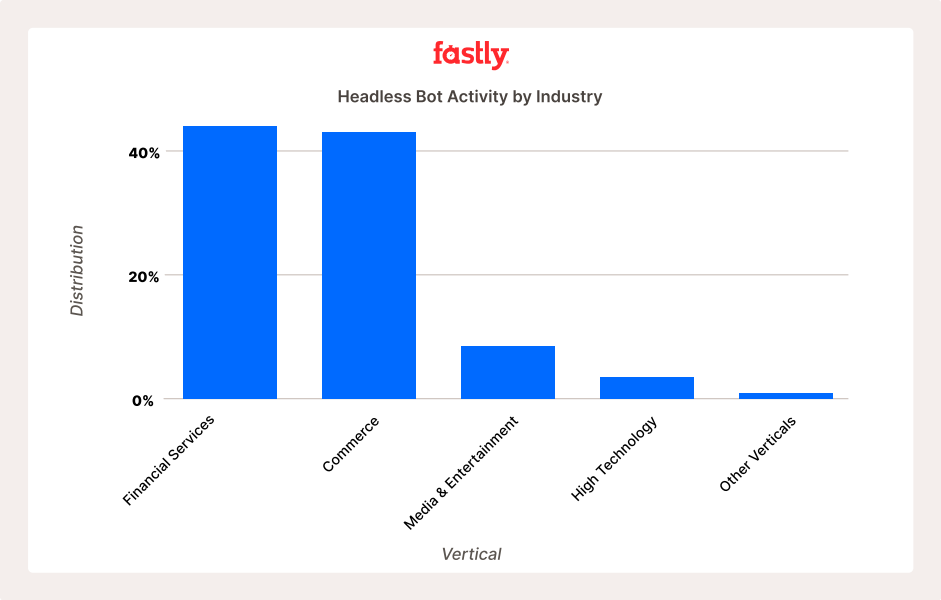
Upon further review, we noted that 'Common Headless Automation' accounted for 94% of total headless bot traffic.

'Common Headless Automation' refers to a collection of widely used browser extensions and tools that interact with websites and APIs. Organizations should place an emphasis on internal policies to identify this type of headless automation usage and prevent unintended blocks from any internal use-cases.



Headless Bots Target Transaction-Heavy Industries

Reviewing Q3 stats, headless bot activity was heavily concentrated among two industries, Commerce (45%) and Financial Services (44%).

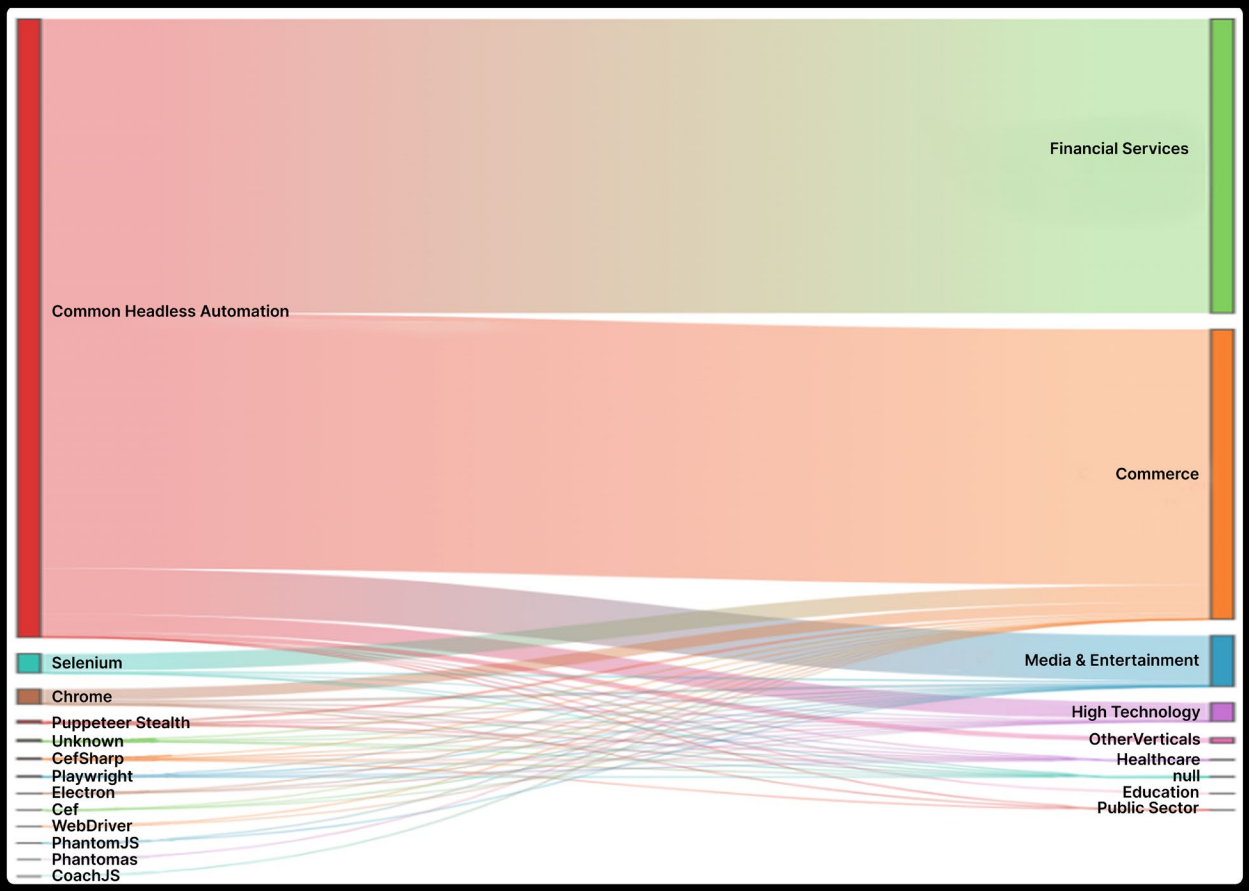


The nature of these two industries makes them appealing for headless bots:

Financial Services institutions and Commerce sites represent opportunities for attackers to compromise accounts, scrape for real-time inventory and pricing data to undercut and snoop on sales – all of which they can do with less security interference under the guise of legitimate traffic via headless clients.

Financial Services and Commerce Spotlight

We combined our views of **headless bot type** with **industry verticals** and yielded several key takeaways.



Financial Services

Financial Services primarily experienced headless bot scraping by the aforementioned ‘Common Headless Automation’ bot classification. We noted no other major headless browser activity.

Financial Services organizations need additional layers of insight into request characteristics and general behavior in order to identify routine activity (like legitimate website monitoring) versus malicious activity. High levels of confidence should be mandatory before organizations take any action around headless bot activity.

Commerce

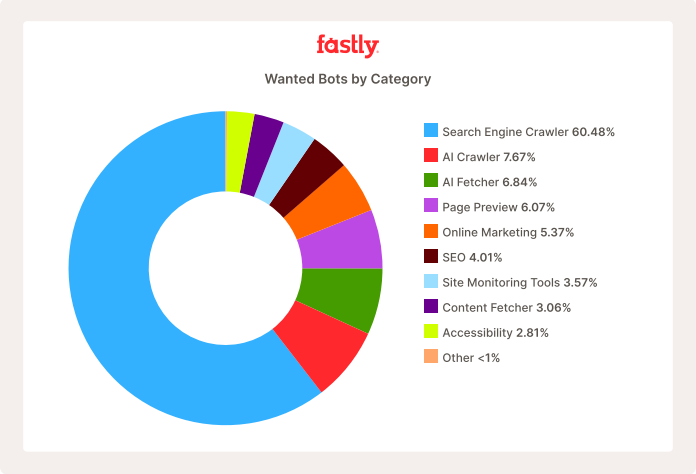
The commerce industry experienced the second-highest volume of headless bots and saw a higher variation, seeing everything from Cef, to Electron, and Selenium bot classifications. This shows a wider variety of bots are targeting these industries, perhaps due to the breadth of different commerce data that can be used.

Wanted Bot Trends

The State of Wanted Bots

The market is shifting to generative engine optimization (GEO) and answer engine optimization (AEO) away from more traditional search engine optimization (SEO). With a recent study showing 80% of consumers now rely on AI summaries for at least 40% of their searches [resulting in a reduction of] traditional website clicks by up to 25%, web owners must optimize their content to show up in AI overviews.

This quarter, **wanted** bots made up 3.56% of all traffic - **this in fact represented trillions of requests in Q3.**



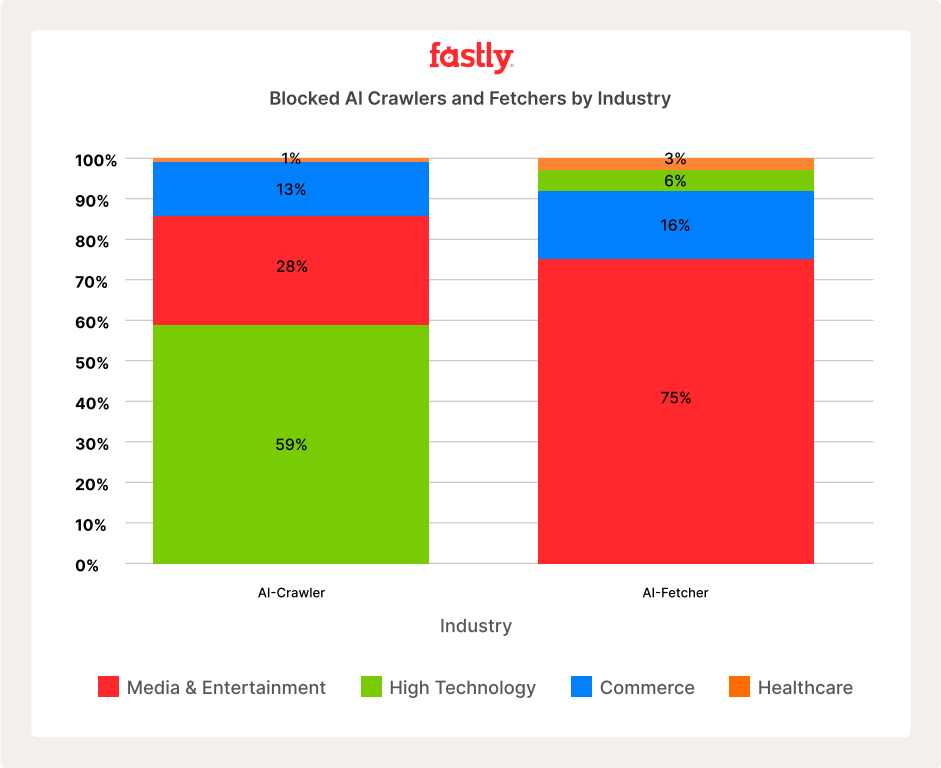
75% is attributable to search engine crawlers, AI fetchers, and AI crawlers, all of which have garnered widespread media attention in the past few years. While a small portion of total traffic, **wanted** bot traffic still has massive implications.

For web owners, this shift to AI content means AI crawlers and fetchers are scouring the internet, scraping their data to form a foundation while fetching in-the-moment insights for the latest content in response to user prompts.

We also found that 4% of all **wanted** bot requests are blocked, indicating that organizations are questioning whether these bots are truly **wanted**. While the data shows we have reached a point where some organizations are taking increased control over which AI crawlers are allowed on their sites, the vast majority are not. AI tolerance is a business decision with clear implications for customer visibility, and ultimately, revenue. Q3 data reveals site owners are increasingly pushing back against this category of bots.

From an industry perspective, 75% of fetcher blocks stemmed from Media & Entertainment organizations, while 59% of AI crawler blocks came from High Technology organizations. The higher percentage of fetcher blocks in Media & Entertainment may reflect generative AI tools use of real time media content to augment their responses and to monetize that content, prompting more aggressive blocking from those media organizations. Alternatively, content from High Technology organizations might be generally useful for training but less critical for real time engagement, resulting in a greater focus on crawlers.

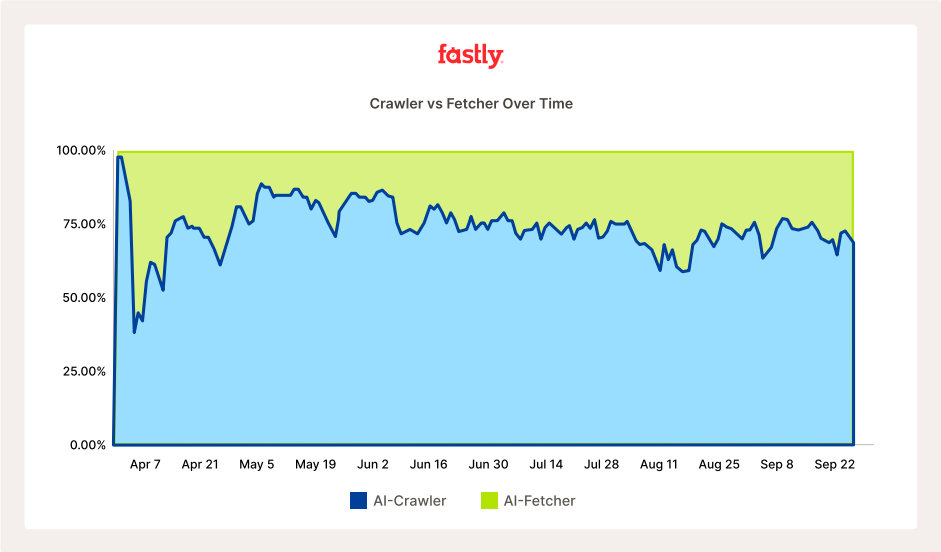
To Media & Entertainment, who are likely seeing diminished referral traffic to their websites thanks to AI overviews, scraping further prevents visitors to their sites, thereby limiting revenue. Both industries are showing lower tolerance of certain AI interacting with their content.



AI Crawler + Fetcher Trends

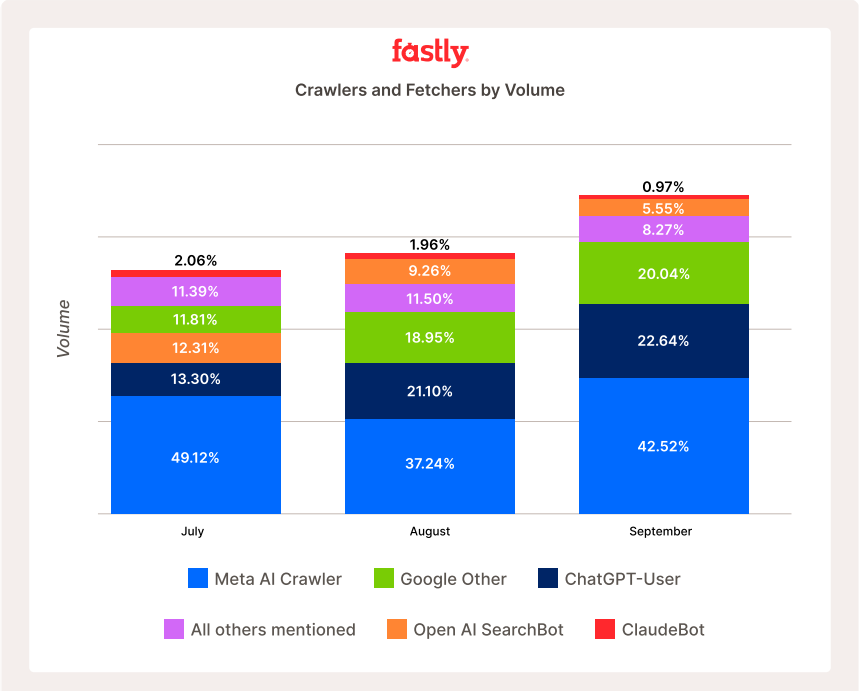
Total Traffic

In this edition, crawler traffic comprised 71% and fetchers, 29%. Examining the traffic distribution over the last two quarters, we observe a steady increase in fetcher traffic. One explanation for this could be the increased usage of AI products like OpenAI's ChatGPT and numerous others. We further examine both categories of wanted bots in the following section.



Bot Type

Examining Q3 AI bot requests over time, Meta's AI Crawler (42.78%), ChatGPT-User (fetcher - 19.41%), and Google Other (Crawler- 17.27%) comprise the highest proportion of the quarter's crawler and fetcher traffic.

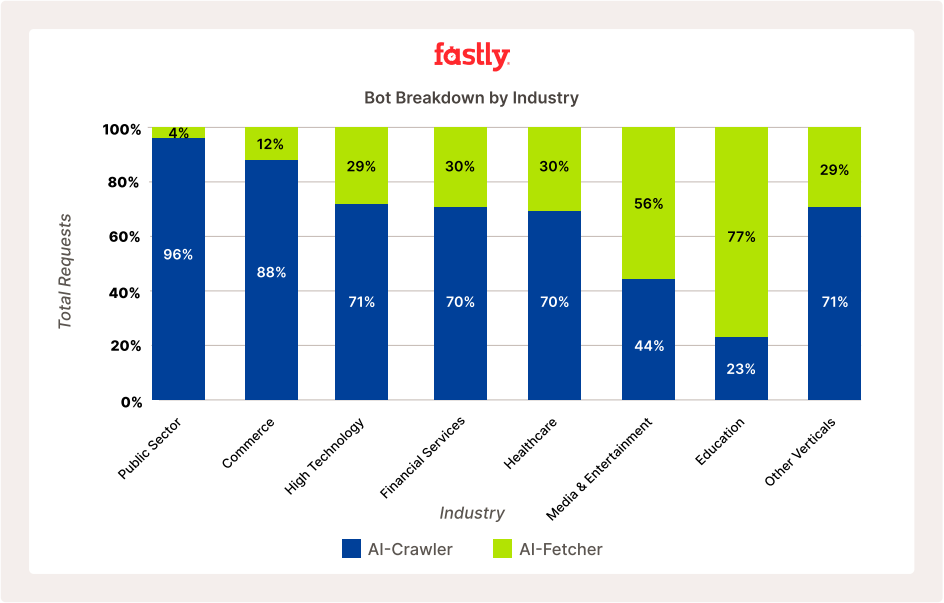


Industry View

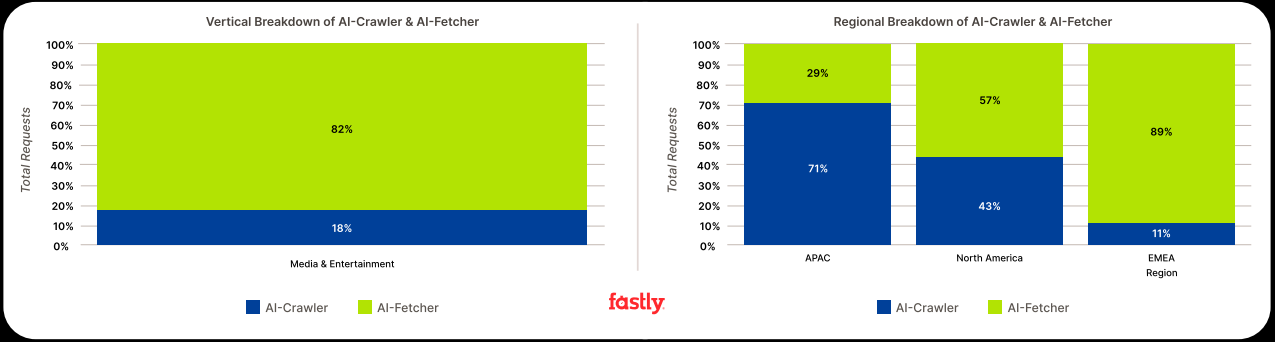
Examining crawlers and fetchers by industry, Commerce (88%) and the Public Sector (96%) verticals received the highest volume of crawler traffic, as a percentage of total. One reason for this is that Crawlers likely have higher demand for scraping of content like product information, which can change quite frequently, necessitating more activity. Similarly, the public sector features high volumes of textual information that is incredibly valuable for an LLM to serve as its corpus while also answering common questions.

In contrast, Education (77%) received by far the highest fetcher volume, as a percentage of total. This may indicate a lack of crawling prioritization, or a strong desire from students for content that is unique or 'fresh', and has therefore not yet been crawled. Course websites are often refreshed every semester; therefore, fetching makes sense, as crawler knowledge might pull less relevant information from prior years.

It could also be that AI fetchers are pulling citations from educational sources - something we may explore in future editions.



Media & Entertainment Spotlight – Publishers



Looking at the Media & Entertainment vertical, we focused on Publishers, given that they're one of the hardest hit by bot traffic.

Through the lens of GEO, all organizations are under immense pressure to adapt, but this is especially true for Publishers. These organizations are often highly reliant on visitors on their sites to view advertisements or pay for access through content gates. Studies show that GEO is creating a world where fetcher referrals occur at a much lower volume than overview consumption.

AI serving content from within its own environment means users are getting the information without visiting the source site. In fact, a recent study showed that only 8% of users, when presented with an AI overview for their query, actually clicked through to the source website. Only 1% in the same study clicked on a source link within the actual AI summary itself, meaning even websites cited within AI overviews get negligible click-through traffic to their sites.

AI overviews most often provide most information the user is looking for, meaning no 'click' through to the source site. In response, publishers must find new ways to adapt and capture this lost traffic, like forcing AI agents to enter pay-per-crawl agreements for access to their content.

Looking at Publisher traffic - by all regions - total crawler traffic came in at 18%, while fetcher traffic was 82%, affirming this trend toward AI Overviews influencing how the 'freshest' Publisher content is consumed. This finding represents an opportunity to collaborate cross-functionally with other parts of your organization to support their strategy. Optimizing content to ensure the use of keywords that match how that content may be searched for can help content rank in AI overviews and ensure the organization is part of the conversation.

By Region

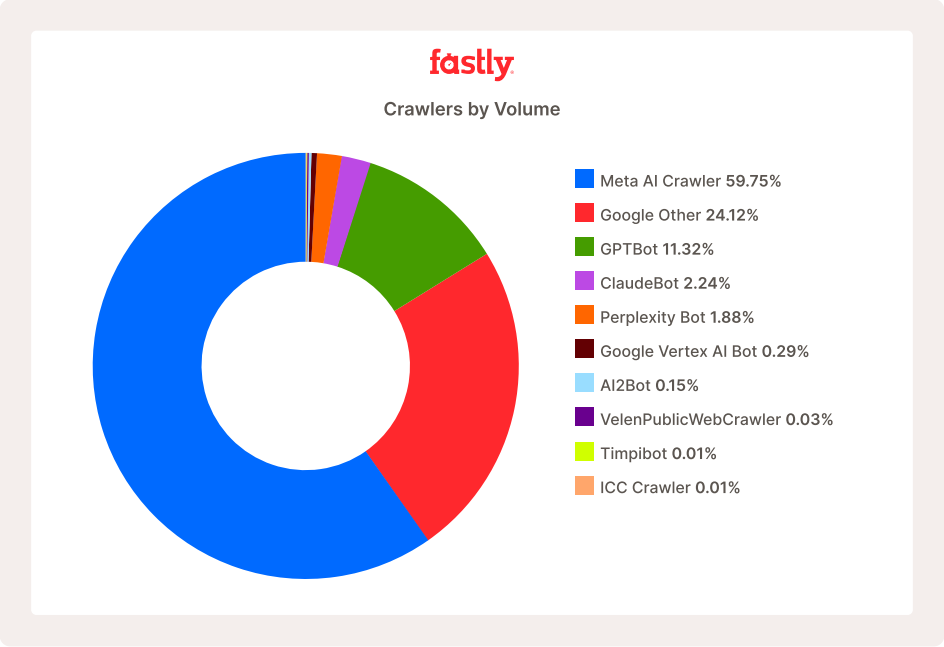
In North America, Publishers saw a 57% to 43% split between crawlers and fetchers, and Media & Entertainment saw crawlers at 73%, and fetchers at 27%. With publishers aiming to deliver timely and in-the-moment content, the higher fetcher traffic makes sense.

Regional data shows vastly different traffic stories, where Europe, Middle East and Africa (EMEA) saw the highest proportion of fetchers (89%) to crawlers (11%). Looking at Publishers over the past two quarters, only 37% has been for crawlers, which limits the foundational data available to a model, and forces them to fetch more relevant content.

Asia-Pacific (APAC) saw the highest percentage of crawler traffic at 71% crawler, 29% fetcher.

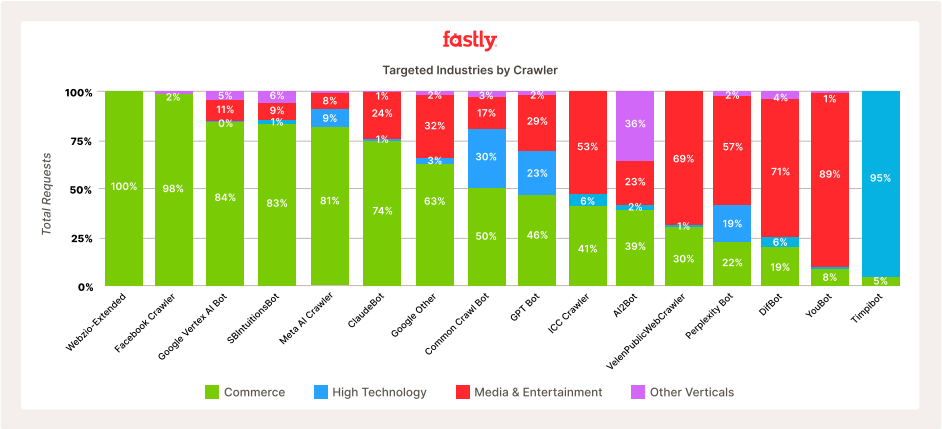
Crawler Deep Dive

Meta's AI crawler was again the most prevalent AI crawler, representing 60% of all AI crawler requests this quarter. Meta's AI crawler having the highest share of crawler traffic is consistent with last quarter's findings, where it also had the highest share, albeit at a relatively lower 52% of total crawler traffic.



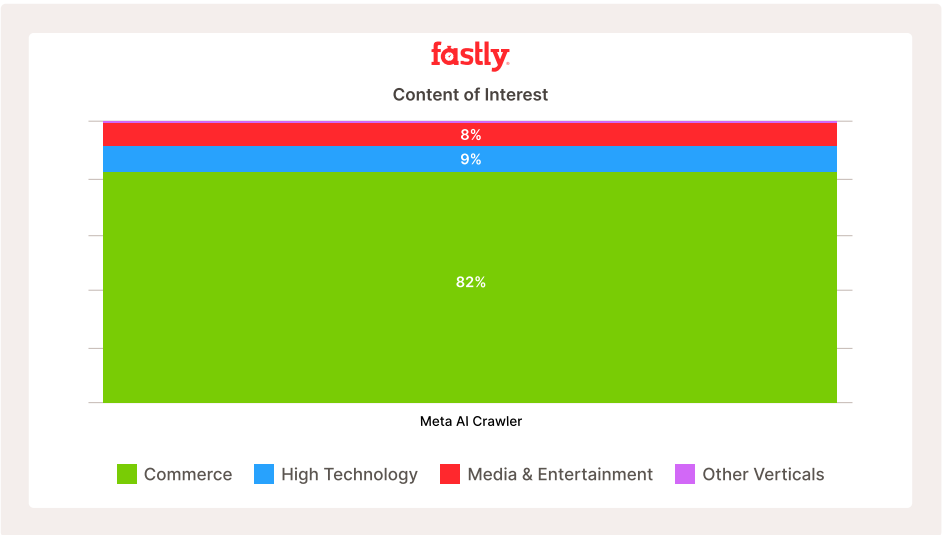
Crawlers by Industry

Looking at the industries hit hardest by crawlers, Commerce is the clear standout as the primary target for most crawler types.

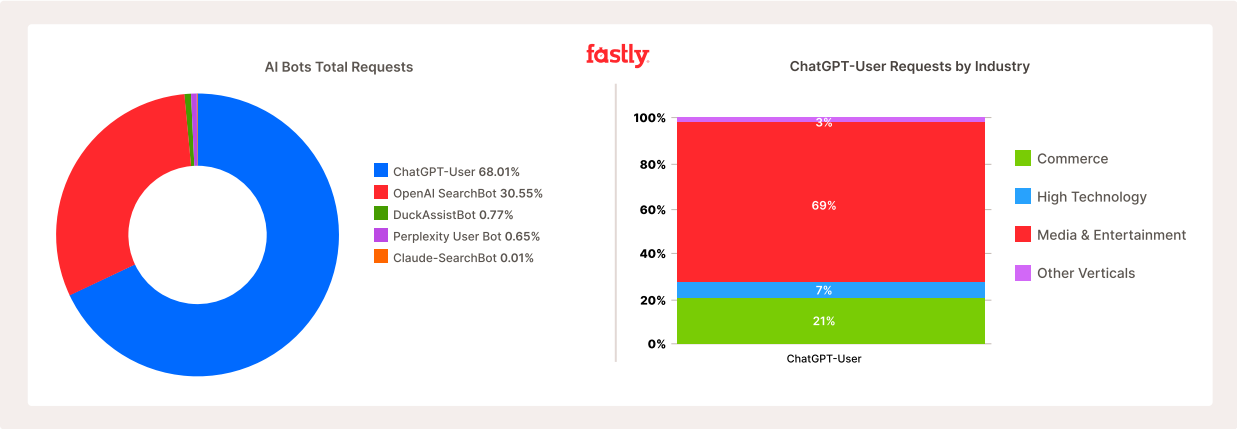


While commerce saw the most crawling volume, these customers experienced a peak crawler velocity of 117 RPS in Q3, which, while large, fell behind that of High Technology and Media & Entertainment (200 RPS and 133 RPS, respectively). This indicates a longer-term interest in content from this industry as opposed to a shorter-term period of increased velocity as seen in High Technology and Media & Entertainment.

Much of Commerce's volume can be attributed to Meta's crawler, which holds the highest distribution of crawled traffic and had a clear affinity for Commerce data in Q3.

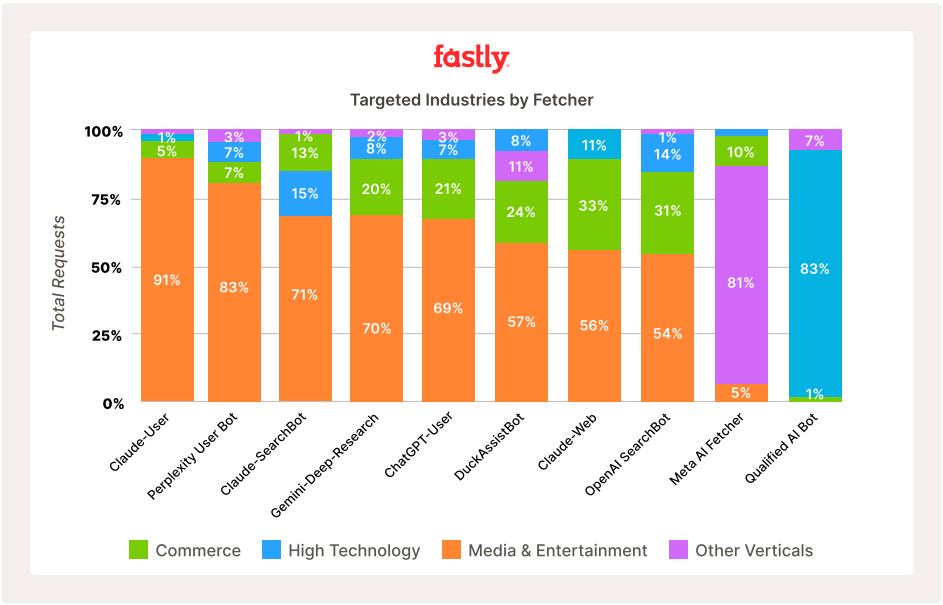


Fetcher Deep Dive



ChatGPT User makes up the highest proportion of fetcher volume and is most heavily impacting the Media & Entertainment industry (69% of total ChatGPT fetcher traffic).

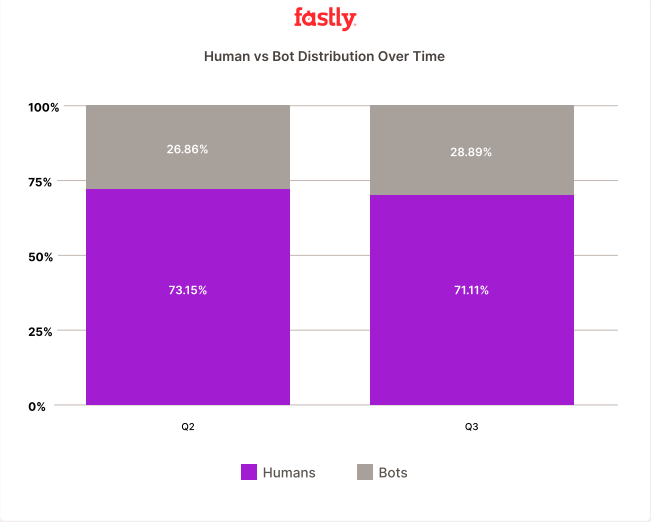
As a percentage of total, the figure below shows where other fetchers are focused. Fetching primarily hits industries with highly dynamic content where crawling may not be possible or where content quickly goes 'stale' (e.g., news articles).



How Crawling and Fetching Trends Should Shape Future Planning

The State of Wanted Bots

Crawlers and fetchers are here to stay, and their volume of requests will only continue to increase if the trends we are tracking persist. Comparing the distribution of bot traffic to human traffic across Q2 and Q3, we see that the increase in bot traffic (combining **wanted** and **unwanted** traffic) was approximately 2%; 26.56% in Q2 2025, versus 28.89% in Q3 2025. While a small percentage of total traffic, influencing distributions of this scale requires billions of requests.



Regardless of how this distribution evolves, we can say with certainty that bot traffic isn't going anywhere. This means establishing a plan to strategically monitor and manage it is no longer optional. When bots account for even small portions of overall traffic, they can still put undue strain on infrastructure, demanding a modern bot management solution.

Fastly Bot Management is trusted by customers across industries to provide the visibility and control needed to distinguish between helpful and harmful bot activity in real time. When it comes to bot operators, transparent intent, verifiable identification, adherence to standards, and responsible crawling can help strike a balance between innovation, fair content use, and preserving control for website owners. Ultimately, adapting to this evolving landscape will be key to safeguarding digital assets and unlocking new opportunities.

If you need help, contact us

Methodology

Some bots provide clear verification mechanisms, such as publishing IP ranges or supporting reverse DNS checks, that make it straightforward to confirm the authenticity of their traffic. In these cases, impostor traffic is easily distinguished and has been excluded from the dataset used in our analysis. However, not all bots offer this level of transparency. For bots lacking public verification data, we rely on alternative heuristics such as the originating network, behavioral patterns, and other identifiable traffic signatures to assess authenticity. While these methods are generally effective, they do not offer absolute certainty. We have worked to ensure the accuracy of the classification and the integrity of the data presented. We encourage bot operators to adopt transparent verification practices to improve attribution.
We have also chosen not to reclassify general-purpose search engine crawlers as AI bots. This is a deliberate decision to avoid misleading conclusions, particularly since blocking such crawlers could unintentionally impact a website's visibility in the associated search engines. To protect the privacy of our customers and avoid unintentionally singling out individual websites, certain details have been intentionally excluded or aggregated in the visualizations and analysis presented in this report. Fastly serves a significant portion of the web, giving it a global perspective on bot activity. This report focuses on overarching patterns in bot behavior, rather than on any individual site or service.

Definitions

Name	Definition
Account Takeover (ATO)	A type of attack to gain unauthorized access to a user's online account through various means, but typically using stolen login credentials.
Bot Traffic	Any non-human internet traffic can be beneficial (e.g., search engine crawlers) or malicious (e.g., carding).
Distributed Denial of Service (DDoS)	An attack that aims to make a website or service unavailable to legitimate users by overwhelming it with traffic.
Unwanted bots	Unwanted bots account for a significant portion of internet traffic, generated by automation tools that provide no business value to websites. Many of these bots are malicious, posing risks such as fraud, data scraping, account takeovers, and infrastructure strain.
Wanted bots	Wanted bots are legitimate automation tools that send requests to websites, typically in ways that benefit the site. Fastly maintains a curated list of these bots, organized by their specific purposes. These bots play an essential role in many online functions, including search engine indexing, site performance monitoring, and security.
Headless Bots	A headless bot is an automated program that runs without a graphical interface, performing tasks in the background. It can interact with websites, APIs, or other systems, simulating a human interaction often for data scraping, automated product purchase, account creation, account takeover, etc.
Web Application Attacks	Techniques and methods attackers use to exploit vulnerabilities in web applications and APIs
Common Headless Automation	Common Headless Automation refers to a classification of headless bots. They are a collection of widely used browser extensions, programs and tools that interact with websites and APIs.