2023 Enterprise Bot Fraud Benchmark Report

An inside look at the bot attack and fraud trends impacting enterprise organizations online

HUMAN

2023 Enterprise Bot Fraud Benchmark Report

Table of Contents

What could you do if you looked like a million humans?

→ That is the question that cybercriminals and fraudsters think about every day. And the possibilities are endless. Bots—software applications that run automated tasks over the Internet—have come a long way from the simple click farms of the past. Today's bots are highly sophisticated, programmed to mimic human behavior, rotate IP addresses, and hide among legitimate users to evade detection. Many sophisticated botnets are even created through malware delivery, which turns an unsuspecting user's device into an internet relay for conducting automated attacks on businesses.

Furthermore, the cost of letting bad bots and fraud go undetected is growing. HUMAN's Satori Threat Intelligence and Research Team has observed bots performing human-like behaviors, such as taking over accounts, making fraudulent purchases, scraping proprietary content, inflating engagement with media, and scalping hot products. One bad bot can cause trouble, but a million bad bots deployed through a sophisticated botnet can wreak havoc and have a material impact. This escalating risk is often unaccounted for. Bot attacks were previously seen as a relatively inconsequential type of online fraud, and that mentality has persisted even as threat actors have gained the ability to cause significant damage to revenue and brand reputation. These are the types of bot attacks and fraud that HUMAN protects against every day.

Malicious bots hide in the shadows of the internet, and HUMAN brings them to light. Illuminating and observing automated attack patterns is the first step in combating this massive threat. Organizations must understand the full scope of the problem in order to solve it. HUMAN's annual Enterprise Bot Fraud Benchmark Report details automated attack patterns against enterprises across the web. These unique insights are based on data gathered from the Human Defense Platform, which verifies the humanity of more than 20 trillion digital interactions per week.

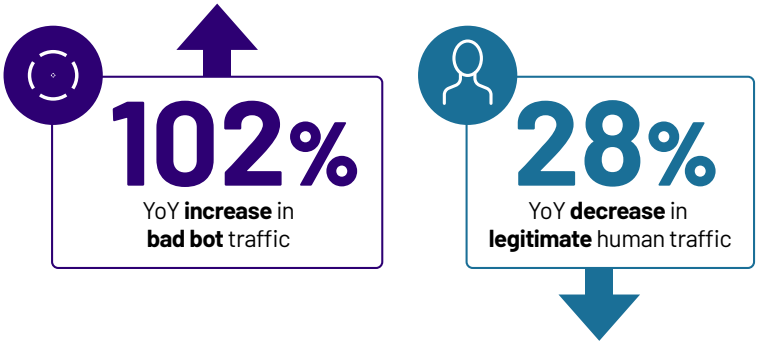
1.

Executive Summary

The annual HUMAN Enterprise Bot Fraud Benchmark Report provides insights into automated attack trends across enterprise use cases, including account takeover, brute forcing, carding, credential stuffing, inventory hoarding, scalping, and web scraping. Here are the key takeaways:

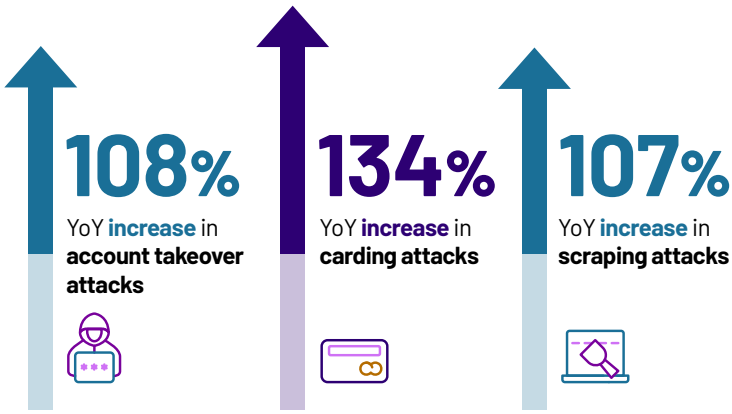
Bad bot traffic overall increased even as people spent less time online

Legitimate human traffic dropped 28% YoY, but bad bot traffic increased 102% YoY — meaning that the percentage of bad bots out of overall traffic has increased even faster.



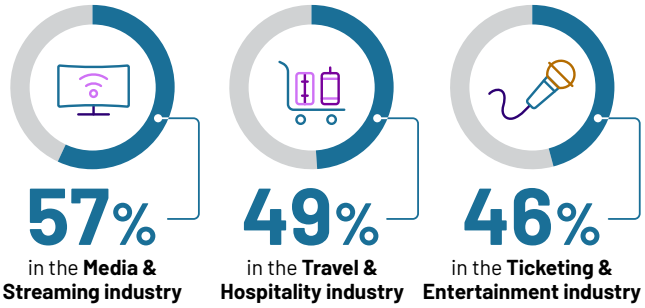
Automated attacks continued to grow

Web applications experienced a YoY increase in three common types of bot attacks. Carding attacks rose 134% YoY, account takeover attacks rose 108% YoY, and scraping rose 107% YoY.



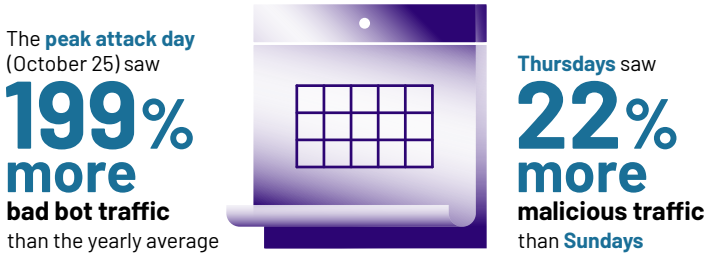
Certain industries experienced more bot attacks than others

Bad bots accounted for 57% of traffic to online businesses in the Media and Streaming industry. Just under 50% of traffic to companies in the Travel and Hospitality industry (49%) and the Ticketing and Entertainment industry (46%) was automated.



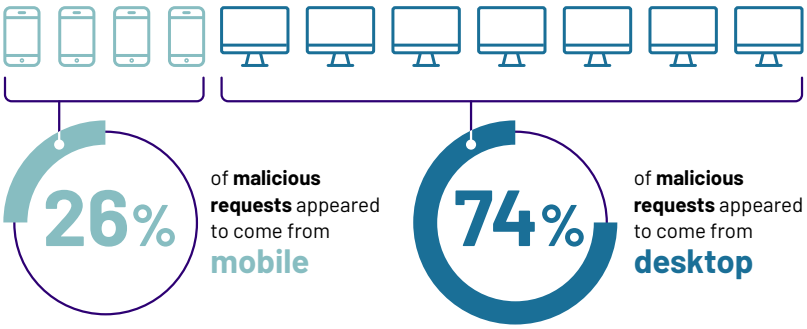
Bad actors conducted more bot attacks during top shopping periods

The holiday shopping season drew more automated attacks than the rest of the year; the peak day (October 25) saw 199% more bad bot traffic than the yearly average. Thursdays saw 22% more malicious traffic than Sundays, the most bot-free day.



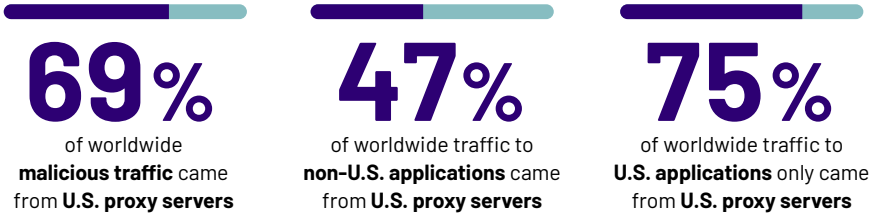
Enterprise attackers prefer to hide behind desktop devices

26% of malicious requests appeared to come from mobile, as compared to 61% of legitimate requests.



Attackers will typically utilize proxy and anonymizing servers in the region they target

More than 69% of worldwide malicious traffic came from U.S. proxy servers. That number drops to 47% when looking only at traffic to non-U.S. applications, and grows to 75% for traffic to U.S. applications only.

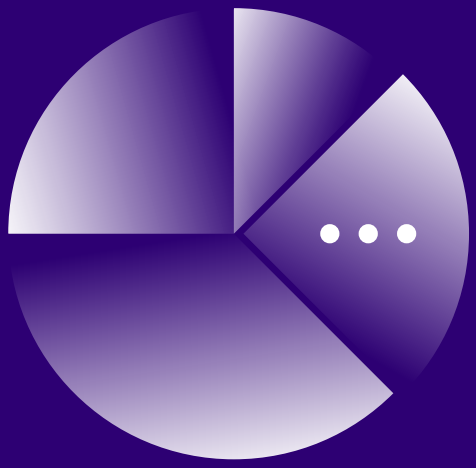


2.

Methodology

The information in this report is based on a sample of the more than 1.5 trillion digital interactions across hundreds of applications, infrastructure elements, and endpoint devices in 2022, as verified by HUMAN. This is a subset of the 20 trillion online interactions that HUMAN observes each week. The data was pulled from the interactions we see and protect on behalf of our customers. Researchers used an out-of-band process, so there was no impact on the performance of monitored traffic or applications.

This report focuses on enterprise bot attacks, including account takeover, brute forcing, carding, credential stuffing, inventory hoarding, scalping, and web scraping. Data was analyzed from organizations in the following industries: education; financial services; food and beverage; healthcare; media and streaming; real estate; retail e-commerce; services, directories, and consulting; technology and SaaS; ticketing and entertainment; and travel and hospitality. The data was anonymized to preserve privacy, and any confidential company data was removed. Note that the data in this report has been normalized; the 25th percentile of outliers have been removed so as to not skew the results.



3.

Overall Traffic Trends

→ Our data show that **legitimate traffic decreased 28% YoY**. The reduction in traffic is likely due to pandemic-era restrictions being lifted, which made people less internet-dependent. Web traffic was at a high in winter 2021, but online interactions dropped as the weather warmed and restrictions eased. We can see that traffic patterns in 2022 are similar to those in the second half of 2021, after the pandemic spike had normalized.

Despite the dip in legitimate traffic, the average percentage of bad bot traffic rose. **Malicious bot traffic rose 102% YoY**. Even as some human activity shifted offline, bad bots continued to attack digital organizations in greater numbers.

"I'll admit I was caught off guard when I saw that web traffic decreased last year. But after further investigation, we can see that this trend is reflected by websites across the board, especially in consumer-facing markets like e-commerce that may have physical locations where customers have the option to interact with brands offline."

-**Gil Bar Yaacov**, Cybersecurity Data Researcher at HUMAN

Legitimate Traffic

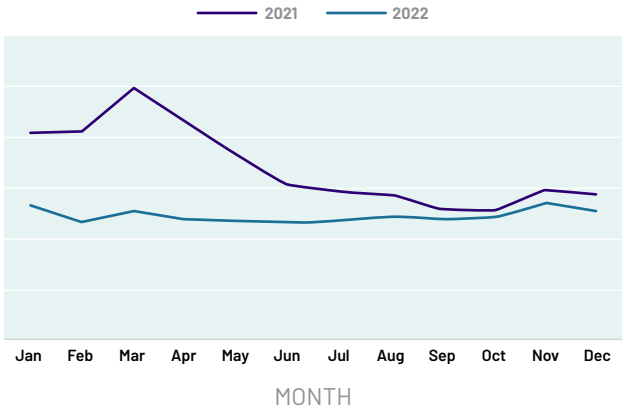


Figure 1: Legitimate traffic to online organizations

Malicious Bot Traffic

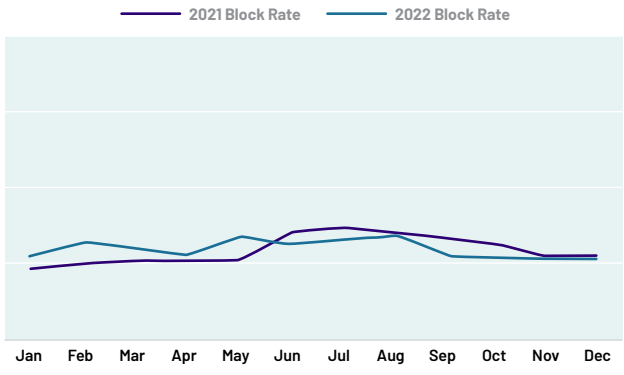


Figure 2: Percent malicious bot traffic out of total traffic

4.

Malicious Traffic Trends

Though bad bot traffic was relatively stable throughout 2022, attacks picked up during the holiday shopping season. This was likely due to an increase in account takeover and carding attacks launched against e-commerce retailers during holiday sales,[1] which peaked in late October and continued through November. **The top attack day (October 25) experienced 199% more malicious traffic than the yearly average**.

Thursday was the number one weekday for bot attacks last year. Overall, **Thursdays saw 22% more malicious traffic than Sundays**, the most bot-free day. It seems that attackers also like to take a day to rest and recharge!

> **"The holiday shopping season continued to be a period of high bot traffic as expected, but attacks actually peaked in October, far before traditional sales days such as Black Friday and Cyber Monday. This is because cybercriminals run automated carding and credential stuffing attacks to validate usernames, passwords, and card numbers in advance of the big sales events. That way, they can be ready with validated accounts and credit cards to use for fraud on top sales days."**
>
> -**Gil Bar Yaacov**, Cybersecurity Data Researcher at HUMAN

Peak Attack Days

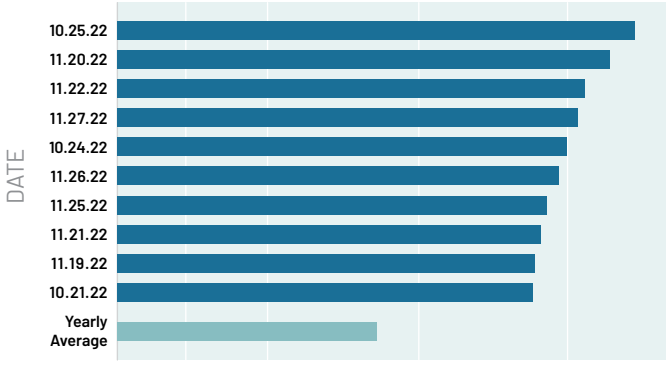


Figure 3: Malicious bot traffic on the peak attack days in 2022

Weekday Bad Bot Traffic

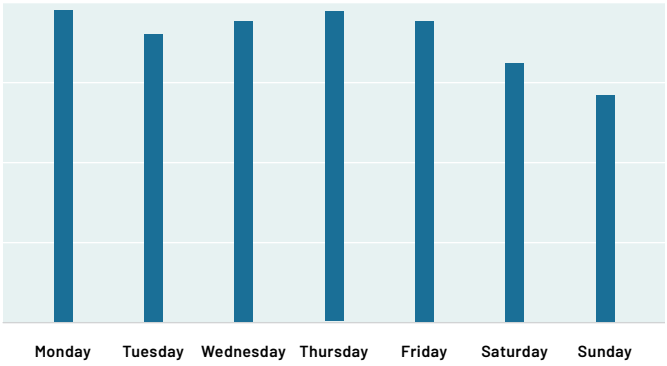


Figure 4: Average amount of malicious traffic per weekday

[1] https://www.humansecurity.com/learn/blog/holiday-bot-trends-black-friday-and-cyber-monday

5.

Malicious Traffic By Country

→ The United States appears to be the global leader in bad bot traffic — "appears" being the key term. Cybercriminals almost always use proxy servers to conduct bot attacks, so looking at web traffic across countries likely describes the location of proxies, not the location of attackers. But the data still tells an interesting story.

Almost 70% of worldwide malicious traffic appears to come from the U.S. However, that number **drops below 50% when we look only at malicious traffic to applications outside of the U.S.** and **increases to 75% when we look only at traffic to applications inside the U.S.** This shows that attackers are using U.S. proxy servers when they want to attack U.S. targets and vice versa (not using U.S. proxies as often when their targets are outside the U.S.).

Proxy Origin (Traffic to Global Applications)

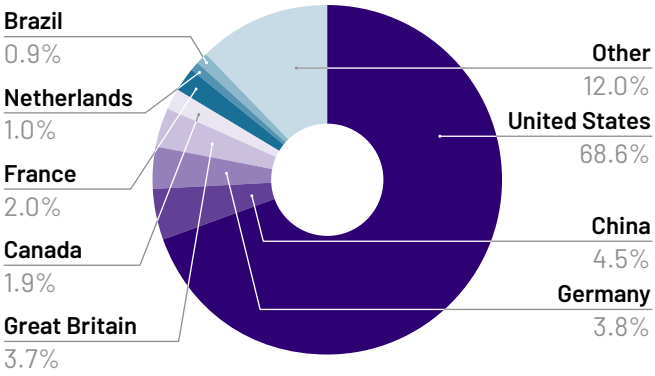


Figure 5: Proxy origin for requests to applications worldwide

Proxy Origin (Traffic to Ex-U.S. Applications)

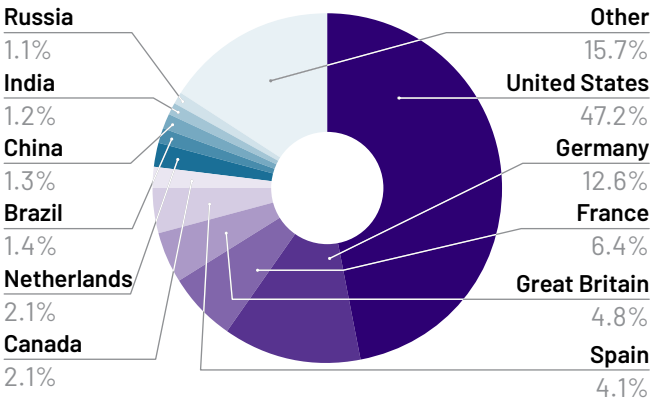


Figure 6: Proxy origin for requests to application outside the U.S.

Cybercriminals strategically pick certain proxies to make fraudulent requests seem more legitimate. While requests from Europe might set off alarm bells to regional U.S. organizations, malicious requests originating from the U.S. might be more likely to blend in with legitimate traffic and fly under the radar. Furthermore, attackers enjoy shorter latency by using proxies closer to their targets, which can be crucial when attempting a high volume attack.

Proxy Origin (Traffic to U.S. Applications)

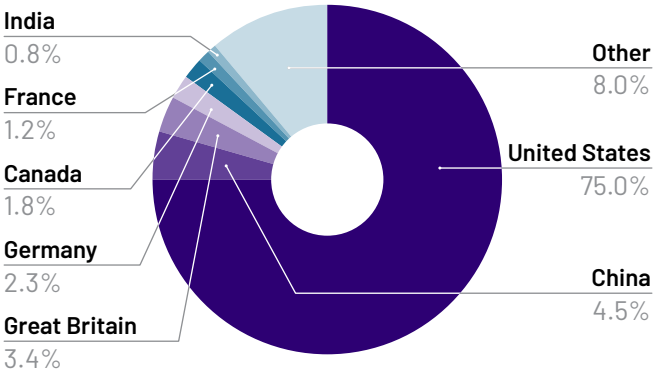


Figure 7: Proxy origin for requests to application inside the U.S.

"At HUMAN, we've seen a steady trend of foreign adversaries using U.S. proxy servers to disguise themselves when targeting web and mobile applications in the U.S. The White House has recently taken action to prevent foreign hackers abusing U.S. cloud servers, and future measures that focus on malicious bots specifically will only strengthen our defenses against bad actors that hide behind U.S. IPs when launching automated attacks."

-**Zach Edwards**, Senior Manager, Threat Insights at HUMAN

6. Traffic by Device Type

Similar to how attackers often fake their locations using proxy servers, attackers also tend to fake their operating system. They do this via the user-agent request header, a characteristic string that lets servers and network peers identify the operating system that a request originates from. In the majority of attacks, it is safe to assume that the user agents are faked. However, it is important to note that attackers are more likely to impersonate operating systems that they are comfortable with.

The device operating system indicates whether the traffic originated from a desktop or mobile device. Last year, **26% of malicious traffic appeared to come from mobile operating systems** (iOS and Android). It seems that bad actors prefer to mimic desktop devices, likely because they are more accustomed to the desktop environment and classic web architecture. Desktop operating systems account for the majority of requests because attackers are familiar with them and know how to impersonate them better, not necessarily because they are actually being used.

On the flip side, legitimate users tended to use mobile devices far more than computers. **More than 60% of legitimate requests came from mobile last year**, and this preference is expected to grow in the future. Despite users' growing preference for mobile devices, the majority of fraudsters are still hiding behind faked desktop devices to commit attacks.

Legitimate Traffic in 2022

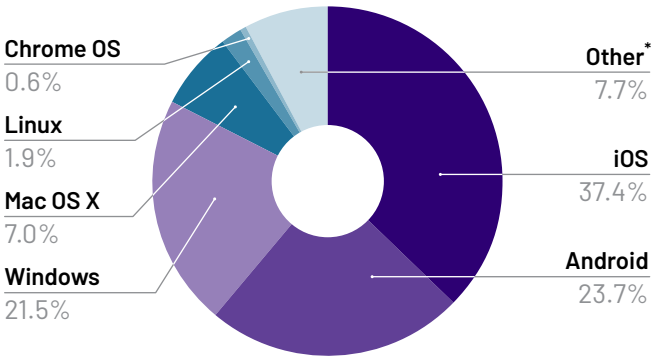


Figure 8: Percent traffic by device operating system (iOS and Android suggest mobile device; Chrome OS, Linux, Mac OS X, Windows, and Other suggest desktop device)

Malicious Traffic in 2022

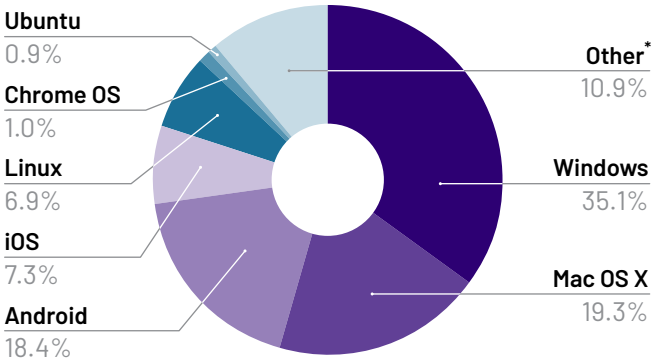


Figure 9: Percent traffic by device operating system (iOS and Android suggest mobile device; Chrome OS, Linux, Mac OS X, Windows, and Other suggest desktop device)

* "Other" category represents the sum of all other OS families that are smaller, obscure, or unknown, including Chrome OS, Windows XP, Windows Vista, Fedora, Debian, FreeBSD, OpenBSD, Windows NT, Windows Phone, Symbian OS, Tizen, Bada, BlackBerry OS, and Windows CE

"When it comes to enterprise bot attacks, attackers must have a good understanding of the web architecture of the attacked website, which is simpler and more familiar on desktop. It is also considered simpler to mimic and spoof the attributes and features of a desktop device. This differs for other types of bot attacks, such as ad or click fraud, which require bot operators to focus more on the interconnected JavaScript supply chains that connect websites and apps together with monetization partners."

-**Liel Strauch**, Director of Cybersecurity Research at HUMAN

7.

Automated Attacks

Web applications experienced a YoY increase in account takeover, carding, and scraping bot attacks. There was also an increase in all three attacks in the second half of 2022 as compared to the first.

Account Takeover

Fraudsters gain unauthorized access to online accounts via automated logins with stolen credentials. This allows them to make fraudulent purchases with stored payment data, drain account balances, steal gift cards and loyalty points, write fake reviews, submit fake warranty claims, and distribute spam and malware.

Carding

Attackers use bots to test stolen credit card and debit card data by making small purchases on e-commerce sites. Validated cards are used to make subsequent fraudulent purchases of products or gift cards, which are then converted into high-value goods and resold online.

Scraping

Bots crawl websites to capture pricing information, product descriptions, inventory data, and restricted content. Competitors use the information to gain a competitive advantage. Furthermore, if bad actors repost scraped content, it can damage the original site's SEO rank.

> **"We see a continued increase in many types of bot attacks, including account takeover, carding, scraping. As web and mobile applications hold more data and value, cybercriminals use automation to target them at scale."**
>
> -**Ido Safruti**, CTO at HUMAN

Account takeover (ATO) attacks rose 123% in the second half of 2022 as compared to the first half due to spikes during the summer months and the holiday shopping season. On average, **48% of total login attempts were malicious**. This is **a 108% YoY increase in account takeover attacks from 2021**.

Account Takeover Attacks in 2022

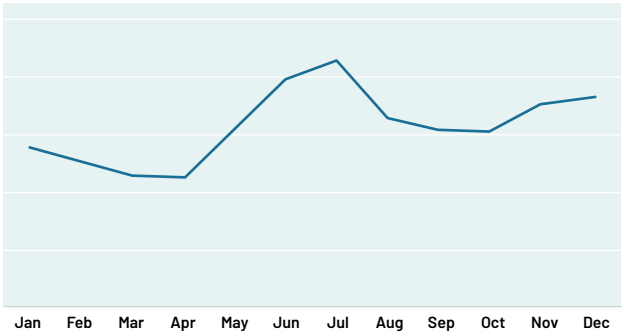


Figure 10: Amount of malicious login requests per month in 2022

Account Takeover Attack Trends

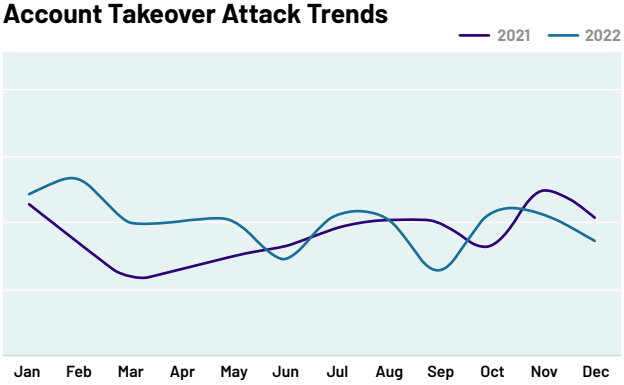


Figure 11: Percentage of malicious login requests out of total login requests

The second half of 2022 saw a 161% increase in carding attacks as the second half of the year compared to the first half. Though carding attacks remained relatively stable throughout the year, there was a significant spike during the holiday shopping season. **Malicious purchase attempts accounted for 11% of all purchase attempts last year**. This was **a 134% YoY increase from 2021**.

Carding Attacks in 2022

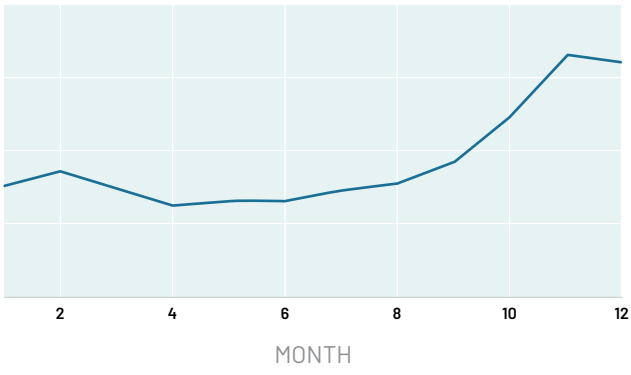


Figure 12: Amount of malicious checkout requests per month in 2022

Carding Attack Trends

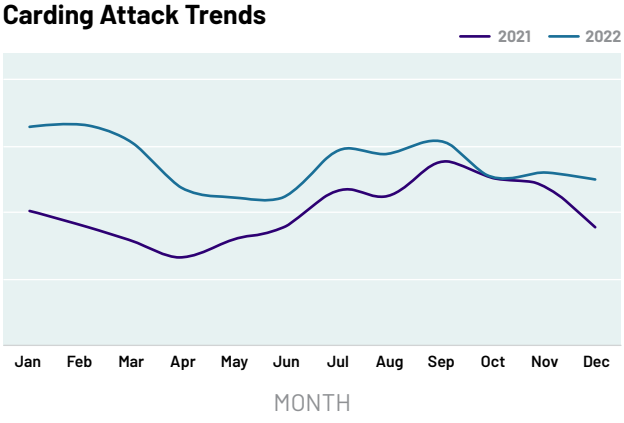


Figure 13: Percentage of malicious checkout requests out of total checkout requests

→ **Scraping attacks grew 112% in the second half of 2022** as compared to the first half. In April, the 9th circuit ruled that scraping was not covered under the Computer Fraud and Abuse Act (CFAA), which likely led to an increase in scraping attacks because bot operators gained newfound confidence that they would not be prosecuted. Other attack spikes are likely due to scraping attacks on travel and hospitality businesses heading into summer, and scraping attacks on e-commerce brands during the holiday shopping season. An average of **34% of total traffic was due to scraping bots last year, a 107% YoY increase**.

Scraping Attacks in 2022

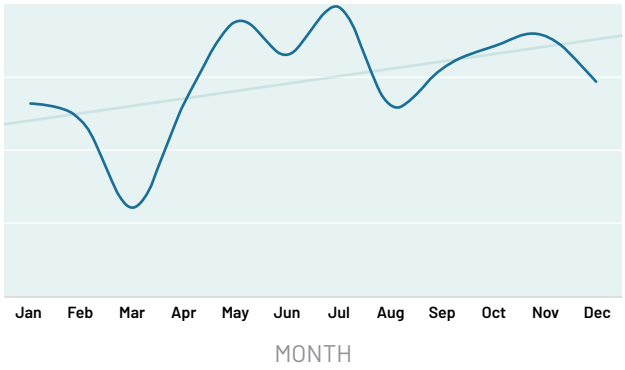


Figure 14: Amount of malicious scraping requests per month in 2022

Scraping Attack Trends

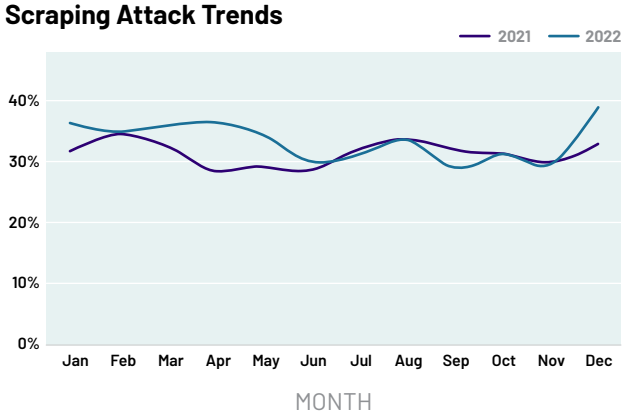


Figure 15: Percentage of malicious scraping requests out of total requests

"Just after the 9th circuit ruled that scraping was not covered under CFAA, HUMAN saw a dramatic increase in scraping attacks across the internet. It was amazing to watch these events unfold in real time."

-**Zach Edwards**, Senior Manager, Threat Insights at HUMAN

8. Malicious Traffic by Industry

Certain industry segments experienced more malicious traffic than others. The top three were Media and Streaming (57%), Travel and Hospitality (49%), and Ticketing and Entertainment (46%). This is likely because each of those industries is a primary target for a certain type of bot attack.

Media and Streaming brands are often targets of account fraud, particularly fake accounts that inflate engagement metrics. These companies tend to offer unique services within the space (for example, the format or genre of media they allow users to stream) and provide a highly specific attack surface with few alternative targets. Attackers create fake accounts en masse to take advantage of signup offers, distribute spam, and prop up/tear down certain media with fake streams, reviews, and comments.

Travel and Hospitality applications are a top target for scraping attacks. Inventory and pricing frequently changes (flight prices increase and decrease, new travel deals are added, etc.), and this is at the heart of business strategy. Product and pricing models supply the competitive edge for travel and hospitality brands. Competitors and bad actors use bots to continually scrape websites and get access to this competitive information as soon as inventory changes.

Ticketing and Events platforms garner a lot of attention, making them a huge draw for scalping bots. And because crowds flock to ticketing providers, bots can easily hide among the noise to evade detection. Scalpers know that hot tickets can easily be resold for a profit on secondary markets, and bots can snatch them up so quickly that real human buyers don't stand a chance.

Bot Traffic by Industry

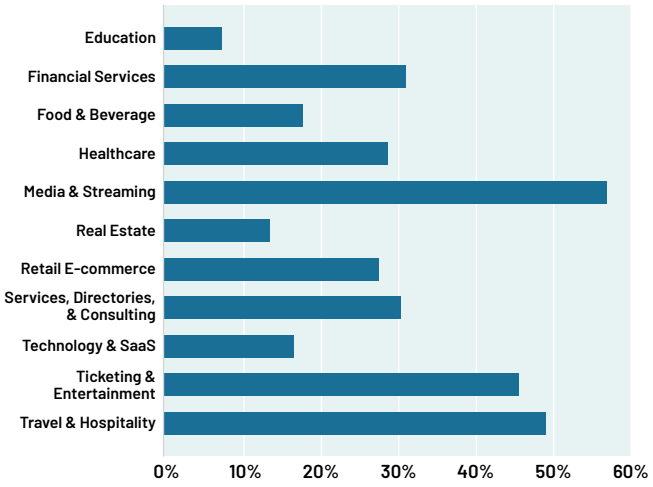


Figure 16: Malicious bot traffic out of total traffic to online businesses in different industries

"The industries mentioned earlier have effectively identified the risks bots pose to their businesses and users. As a result, they have improved their ability to detect and comprehend unauthorized traffic and potential attacks. However, other sectors not mentioned here, such as critical infrastructure and government websites, lack this awareness, making it difficult to determine the actual scope of bot activity. To fully comprehend their challenges and implement appropriate protective measures, online entities must gain visibility into automated traffic."

-**Gavid Reid**, CISO at HUMAN

9.

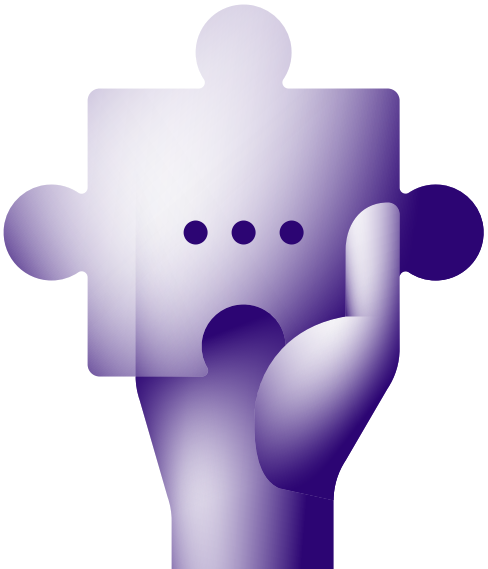
Summary: HUMAN Insights

As pandemic restrictions eased in many places and people spent less time online, web traffic stabilized. In 2022, we saw more steady trend lines in regards to bot attacks, fraud and traffic trends across the board. This has allowed us to provide more significant benchmarks based on data that was less prone to fluctuations and abnormalities.

In 2023, it seems that unpredictable spikes in bot attacks are unlikely (at least on a year-wide basis) as attacks have become more constant. Certain periods—such as concert ticket release days, Cyber Monday, and days surrounding political events—will always be high targets. However, other seemingly insignificant days are often prone to bot attacks as well. Today, the ebb and flow of bot traffic is better described as just the flow and bigger flow. Bots are a persistent and growing threat, so digital organizations must have defenses in place all year round.

"Looking back on 2022, it's clear that bots are a pervasive threat. It is extremely easy for bad actors to conduct malicious bot attacks and fraud with minimal effort or risk. This means that cybercriminals can take advantage of any event online, big or small — making all events open for attack."

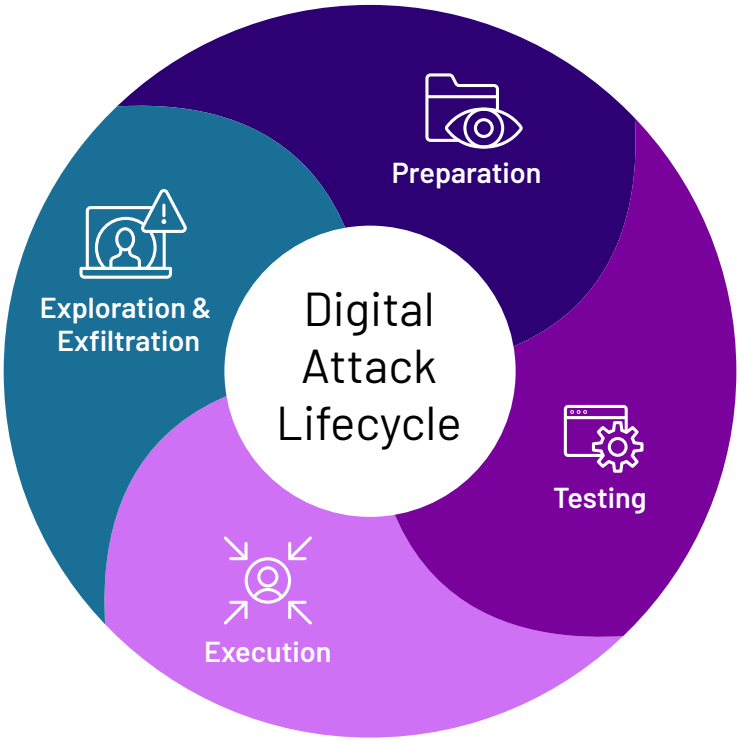
-**Gavid Reid**, CISO at HUMAN



10.

Bots and the Digital Attack Lifecycle

Malicious bots are involved in 77% of all digital attacks, which in turn fuel a wide range of cyberattacks across the digital attack lifecycle. One attack feeds another, such as a PII breach fueling a downstream account takeover attack. In order to ensure complete protection, enterprises must establish end-to-end protection over the entire cybercrime journey.



Preparation
- Data Breaches
- Digital Skimming and Magecart
- Malware
- Phishing and Social Engineering
- PII Harvesting and Formjacking
- Web Scraping

Testing
- Brute Force
- Credential Stuffing
- Carding
- Gift Card Cracking

Execution
- Account Takeover
- Fake Account Creation
- Inventory Hoarding
- Scalping

Exploitation and Exfiltration
- Account Abuse
- PII and Sensitive Data Theft
- Promotion Abuse
- Transaction Fraud

How to mitigate bad bots and online fraud:

Start with good security hygiene and basic defenses, including:

- Using strong passwords
- Keeping software up-to-date
- Enabling HTTPS
- Regularly monitoring and scanning for vulnerabilities
- Configuring proper access controls
- Implementing policies such as Content Security Policy (CSP) and Cross-Origin Resource Sharing (CORS)
- Understanding and testing the data flow from the client to the server
- Knowledge of all the microservices and other related applications and how they interact with the data flow
- Blocklisting/allowlisting

Enable additional security measures specifically geared towards mitigating sophisticated bad bots and fraud that rotate IP addresses and mimic human user behavior, such as:

- Volumetric detection and analysis
- Reverse proxying
- Rate limiting
- Intelligent fingerprinting
- Behavioral analysis
- Advanced machine learning algorithms
- Real-time sensors

Shore up your client-side and post-login account attack surfaces to protect your business and users from threats beyond bots.

- Client-side code monitoring and access control
- Continuous evaluation of user activity post-login

Ensure future-proof protection by not only blocking current threats, but also raising the cost of attacks and reducing the attack surface. For example:

- Compromised credential resets
- Computational challenges (proof-of-work)
- Deceptive content
- Honeypots
- Misdirection

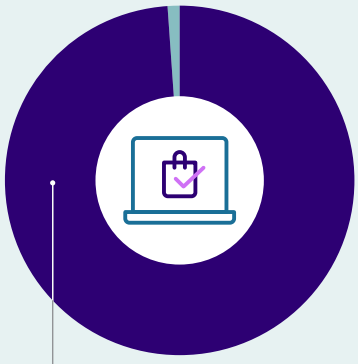
Establish a feedback loop with real-time threat intelligence that continuously strengthens detections and disrupts online fraud.

- Collaborate with the larger security community to disrupt and take down fraud schemes
- Develop a modern defense that takes advantage of sharing threat signals and details about ongoing attacks

11.

HUMAN Disrupts Online Fraud and Abuse

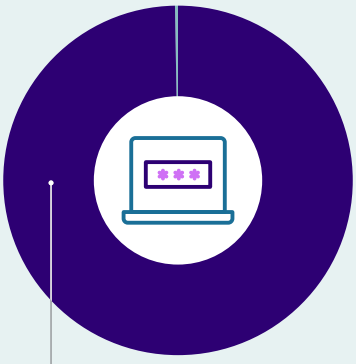
The data in this report represents companies across industries, geographies, and sizes. We have normalized the average findings, but also want to call out some peak attacks that HUMAN witnessed.



In June 2022

99.15%

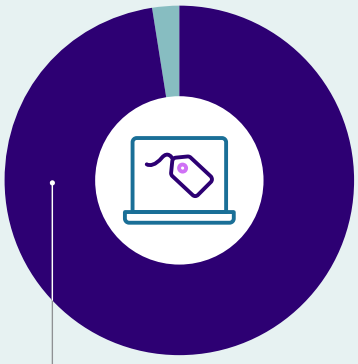
of checkout attempts to one e-commerce retailer were malicious.



In July 2022

99.74%

of login attempts on one financial services platform were malicious.



In October 2022

97.76%

of product views on one SaaS application came from scraping bots.

In all of the above cases, HUMAN was able to stop the automated attacks before fraud was committed.

HUMAN Bot Defender is a behavior-based bot management solution that protects your websites, mobile applications, and APIs from automated attacks. The solution uses more than 300 machine learning algorithms to detect and mitigate bad bots with unmatched speed, scale, and precision. Bot Defender is complemented by a suite of web application security solutions that comprise the Human Defense Platform, which disrupts online fraud and abuse with modern defense.

Modern defense — built on the three pillars of visibility, network effect, and disruptions and takedowns — is the fuel behind everything HUMAN does.

Our unmatched **visibility** allows us to keep on the pulse of cyberthreats across the web, whether that's a bot attack on a single customer or a larger attack hitting multiple organizations. With our **network effect**, we share knowledge and deploy protections for all of our customers. We **disrupt** cybercrime with every mitigation action; we don't just block real-time threats, but execute a range of responses that increase the cost to bad actors and deter future attacks. By using modern defense to disrupt the economics of cybercrime, the Human Defense Platform delivers collective protection to combat tomorrow's cybersecurity threats, today.

Contact HUMAN to see how we can help block bots and disrupt online fraud.

Visibility

Detection at unmatched scale

More than 20 trillion digital interactions are verified per week, and more than 3 billion devices are observed monthly to provide actionable intelligence.

Network Effect

Collective protection across the internet

2,500 dynamic network, device, and behavioral signals are parsed through 350 algorithms (technical, statistical, and machine learning).

Disruptions & Takedowns

Raise the cost of every digital attack

10+ years of experience combating adversary attack vectors, tools, amd methodologies to disrupt cybercrime through takedowns, deception, and other innovations.

> **"When it comes to detection, nobody does it better than HUMAN. They make sure the bots get all the friction without touching the customer experience."**
>
> -**Security Engineer**, Global E-commerce Retailer

About Us

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.