imperva

REPORT

2022 Imperva Bad Bot Report

Evasive Bots Drive Online Fraud

Contents

About the 2022 Imperva Bad Bot Report

Leveraging data from our global network, Imperva Threat Research investigates the rising volume of automated attacks occurring daily, evading detection while wreaking havoc and committing online fraud.

The 9th annual Imperva Bad Bot Report is based on data collected from the Imperva global network throughout 2021. The data is composed of hundreds of billions of blocked bad bot requests, anonymized over thousands of domains. The goal of this report is to provide meaningful information and guidance about the nature and impact of these automated threats.

Bot attacks are often the first indicator of fraudulent activity online, whether it's validating stolen user credentials and credit card information to later be sold on the dark web, or scraping proprietary data to gain a competitive advantage. Often bots are used to surveil applications and APIs in an attempt to discover vulnerabilities or weak security. Online fraud from automated bot attacks is not only a threat to the business, but it is first and foremost a risk to customers. Bad bot attacks might cause customers to be unable to access their accounts or have sensitive information stolen from them due to successful account takeover fraud.

Bad bots mask themselves and attempt to interact with applications in the same way a legitimate user would, making them harder to detect and block. They enable high-speed abuse, misuse, and attacks on your websites, mobile apps, and APIs. They allow bot operators, attackers, unsavory competitors, and fraudsters to perform a wide array of malicious activities.

Such activities include web scraping, competitive data mining, personal and financial data harvesting, brute-force login, digital ad fraud, denial of service, denial of inventory, spam, transaction fraud, and more.

Definitions

What is a bad bot?

Bad bots are software applications that run automated tasks with malicious intent. They scrape data from sites without permission to reuse it and gain a competitive edge (e.g. pricing, inventory levels, proprietary content). They are used for scalping, the act of obtaining limited availability items to resell at a higher price. They can be used to create distributed denial of service (DDoS) attacks targeted at the network or the application. The truly nefarious ones undertake criminal activities, such as fraud and outright theft. Credential Stuffing to perform Account Takeover is a prominent tactic of bad bots. The Open Web Application Security Project (OWASP) provides a comprehensive list of 21 different bad bot use cases in its Automated Threat Handbook.[1]

What is the difference between good and bad bots?

Not all bots are bad and there are many examples of good bots that provide beneficial services. For example, good bots are used to discover and make online services and content available to search engines. This ensures that online businesses and their products can be easily found by prospective customers. Examples include search engine crawlers such as Googlebot and Bingbot that, through their indexing, help people match their queries with the most relevant sets of websites.

Recognizing the difference between good and bad bots is essential in a bot prevention solution, but it is becoming harder as bad bot behaviors become increasingly sophisticated. A layered defense model that accounts for various user behaviors and includes user profiling and fingerprinting keeps the good bot benefits while filtering out the bad bot activity.

Bad bot classification levels

Imperva created the following classification system that categorizes bad bots by their level of sophistication:

Simple – Connecting from a single, ISP-assigned IP address, this bot connects to sites using automated scripts, not browsers, and masquerades – doesn't self-report – as a browser.

Moderate – This more complex bot uses "headless browser" software that simulates browser technology, including the ability to execute JavaScript.

Advanced – Producing mouse movements and clicks that fool even sophisticated detection methods, these bots mimic human behavior and are the most evasive. They use browser automation software, or malware installed within real browsers, to connect to sites.

Evasive – These are a grouping of both moderate and advanced bad bots. They tend to cycle through random IP addresses, enter through anonymous proxies and peer-to-peer networks, and can change their user agents. They use a mix of technologies and methods to evade detection while maintaining persistence on target sites. They often choose "low and slow" tactics, which enable them to carry out significant attacks using fewer requests and even delay requests, allowing them to not stand out from the normal traffic patterns and avoid triggering rate-based security detection thresholds. This method reduces the "noise," or big traffic spikes generated by many bad bot campaigns.

1. https://owasp.org/www-project-automated-threats-to-web-applications/

Understanding what bad bots do

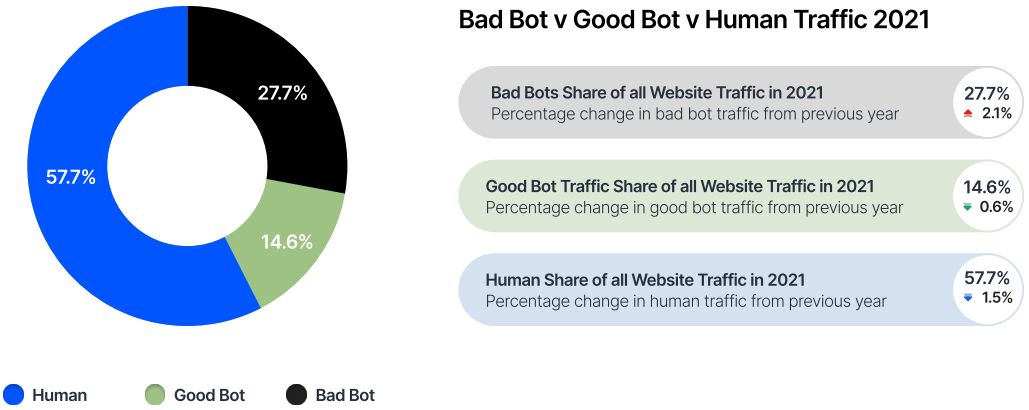
Bad Bot Problem	How it Hurts the Business	Signs You Have a Problem	Industries Targeted
Price Scraping	Competitors scrape your prices to beat you in the marketplace. You lose business because your competitor wins the SEO search on price. The lifetime value of customers worsens.	Declining conversion rates. Unexplained website slowdowns and downtime, usually caused by aggressive scrapers.	All businesses that show prices: • Retail • Gambling • Airlines • Travel
Content Scraping	Proprietary content is your business. When others steal your content they are a parasite on your efforts. Duplicate content damages your SEO rankings.	Your content appears on other sites. Your SEO rankings drop. Unexplained website slowdowns and downtime, usually caused by aggressive scrapers.	Similar to Price Scraping, but in addition: • Job boards • Classifieds • Marketplaces • Finance • Ticketing
Account Takeover (aka Credential Stuffing, Credential Cracking)	Stolen credentials tested on your site. If successful, the ramifications are account lockouts, financial fraud, and increased customer complaints affecting customer loyalty and future revenues.	Increase in failed login rates. Increase in customer account lockouts and customer service tickets. Increase in fraud (lost loyalty points, stolen credit cards, unauthorized purchases). Increase in chargebacks.	Any business with a login page requiring a username and password.
Account Creation (aka Account Aggregation, New Account Fraud)	Free accounts used to spam messages or amplify propaganda. Exploit any new account promotion credits (money, points, free plays).	Abnormal increases in new account creation. Increased comment spam. Drop in conversion rates from new accounts to paying customers.	Messaging platforms • Social media • Dating sites • Communities Sign-up promotion abuse • Gambling
Credit card fraud (aka Carding, Card Cracking)	Criminals testing credit card numbers to identify missing data (exp. date, CVV). Damages the fraud score of the business. Increases customer service costs to process fraudulent chargebacks.	Rise in credit card fraud. Increase in customer support calls. Increased chargebacks processed.	Any site with a payment processor: • Retail • Nonprofit/Charities • Airlines • Travel • Ticketing • Financial • Gambling

Bad Bot Problem	How it Hurts the Business	Signs You Have a Problem	Industries Targeted
Denial of Service	Slows the website performance causing brownouts or downtime. Lost revenue from the unavailability of websites. Damaged customer reputation.	Abnormal and unexplained spikes in traffic on particular resources (login, signup, product pages, etc.). Increase in customer service complaints.	All industries
Gift Card Balance Checking	Steal money from gift cards that contain a balance. Poor customer reputation and loss of future sales.	Spike in requests to the gift card balance page. Increase in customer service calls about lost balances.	Any business offering gift cards as a payment option, Retail predominantly
Denial of Inventory	Bots hold items in shopping carts, preventing access by valid customers. Damaged customer reputation because unscrupulous middlemen hold all inventory until resold elsewhere.	Increase in abandoned items held in shopping carts. Decrease in conversion rates. Increase in customer service calls about lack of availability of inventory.	Businesses offering scarce or time-sensitive items: • Airlines • Tickets • Retail • Healthcare
Scalping (aka Grinchbots, Sneaker Bots, Ticket Bots, Vaccine Bots)	Bots are used to obtain limited-availability and/or preferred goods/services. Damaged customer reputation. Slows the website performance causing brownouts or downtime, leading to loss of revenue.	Website slowdowns, potentially even Denial of Service as a side effect of the many requests to the webserver. Decrease in conversion rates. Increase in customer service calls about lack of availability of inventory.	Similar to Denial of Inventory: • Airlines • Tickets • Retail E.g. sneakers, consoles, computer hardware, limited edition items. • Healthcare

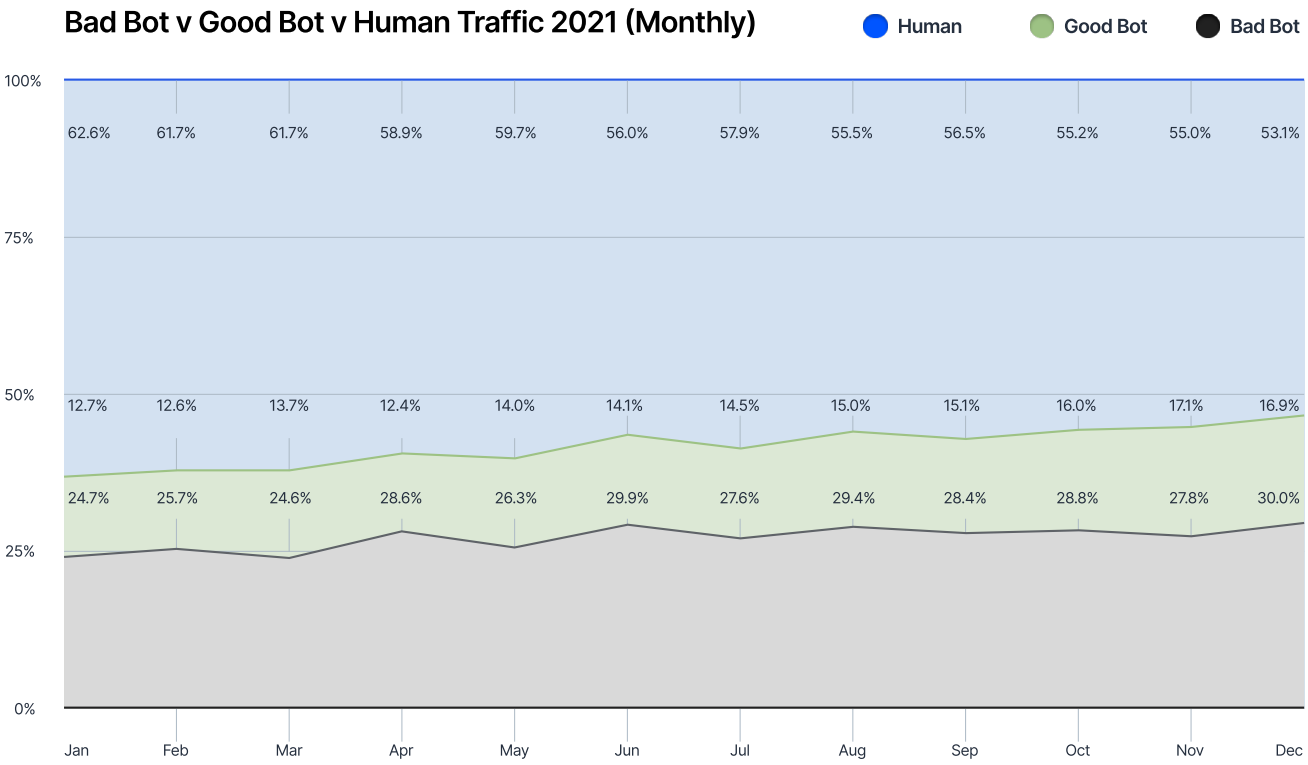
Executive summary of findings

Bad bot traffic continues to grow and hits record levels

Bad bot traffic accounted for a record-setting 27.7% of all global website traffic in 2021, up from 25.6% in 2020. Combined with good bot traffic, 42.3% of internet traffic this past year wasn't human, compared to 40.8% in 2020. Human traffic decreased by 2.5% to 57.7% of all traffic. The top three most common bot attacks in 2021 were Account Takeover, Scraping, and Scalping.

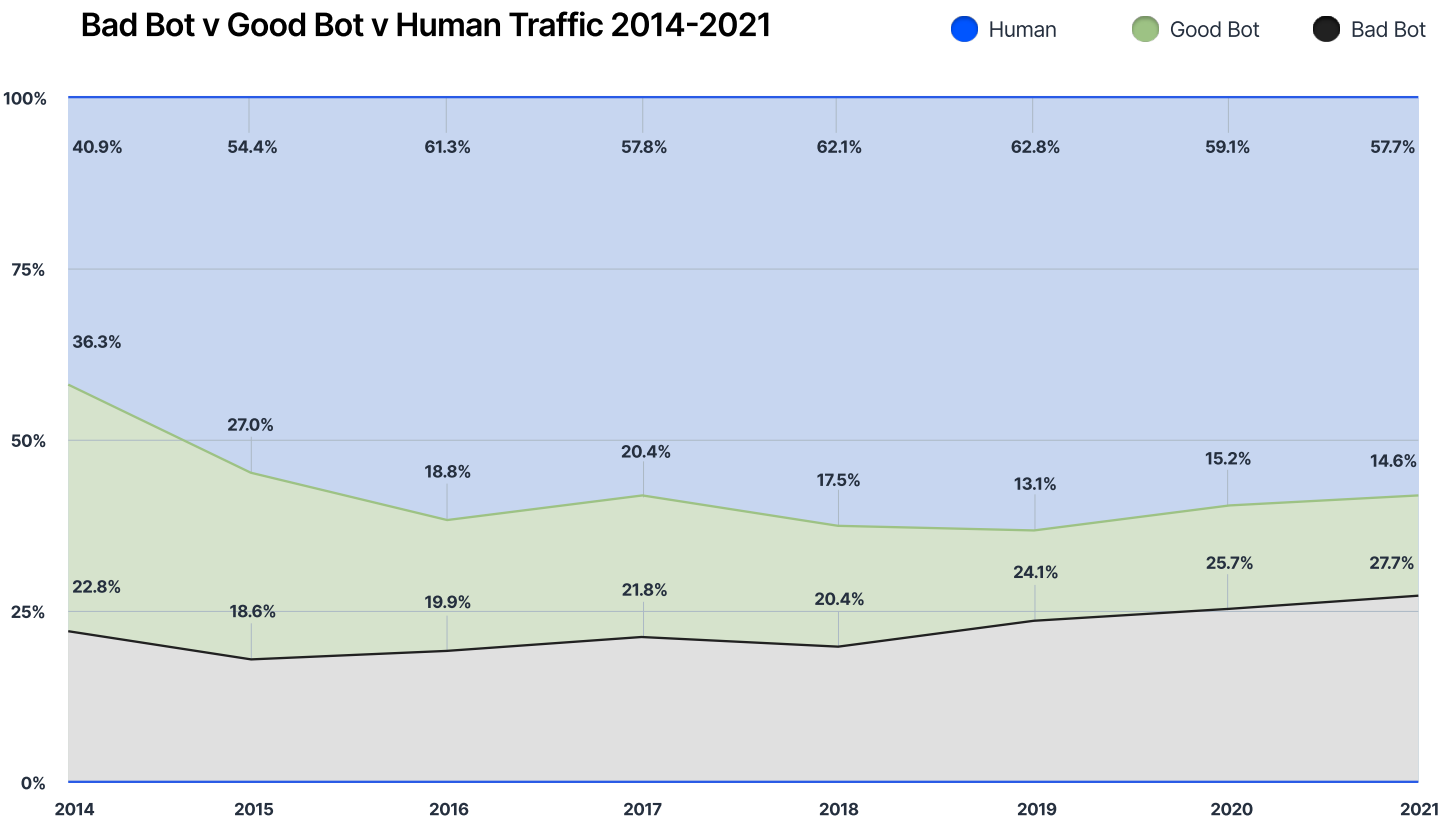


Analyzing the data by month, there is a consistent trend line that indicates a rising volume of bot traffic throughout the year. Bad bot traffic levels increased at the end of the year, accounting for 30% of all traffic in December. The holiday shopping season as well as the emergence of the Log4j vulnerability, which is exploitable by bots, have contributed to that rise in traffic.



2021 was another record-breaking year for bad bot traffic, in comparison to data collected since the inception of the Imperva Bad Bot Report in 2014. This year, bad bots accounted for 27.7% of all traffic across web, mobile, and APIs. That is a 2.1% increase over the previous year.

Both good bot and human traffic ratios decreased with the rise in bad bot traffic. The proportion of good bot traffic accounted for 14.6% of all traffic. With bad bots continuing to trend upwards, the proportion of human traffic is down once again, going from 59.2% in 2020 to 57.7% in 2021. That marks a 2.5% decrease from 2020. One reason for this could be the return to pre-pandemic levels of human internet traffic.

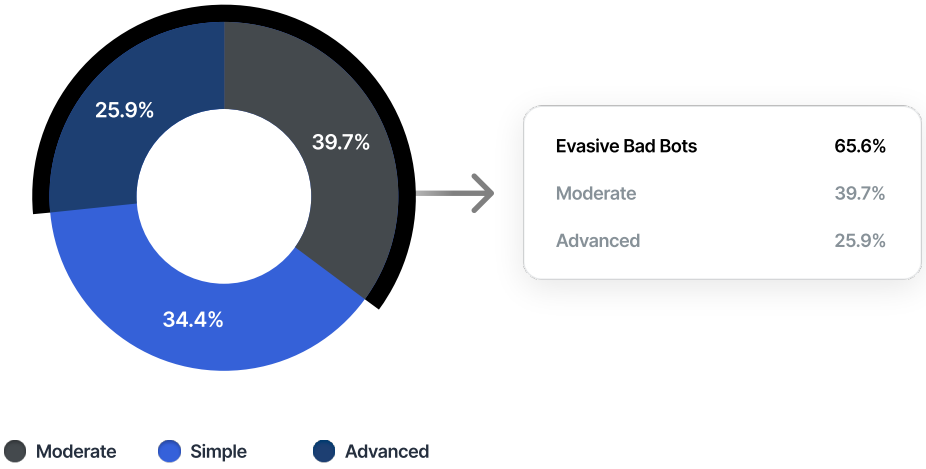


	2014	2015	2016	2017	2018	2019	2020	2021
Bad Bots	22.8%	18.6%	19.9%	21.8%	20.4%	24.1%	25.6%	27.7%
Good Bots	36.3%	27.0%	18.8%	20.4%	17.5%	13.1%	15.2%	14.6%
Humans	40.9%	54.4%	61.3%	57.8%	62.1%	62.8%	59.2%	57.7%

Evasive bad bots are on the rise

Bots continue to evolve and are becoming more sophisticated and designed to evade detection of less sophisticated bot protection solutions. In 2021, Evasive Bad Bots accounted for the majority of bad bot traffic (65.6%). This breed of bot is a grouping of both moderate and advanced bad bots that can evade common defenses. They use the latest evasion techniques, including cycling through random IPs, entering through anonymous proxies, changing their identities, mimicking human behavior, delaying requests, and more.

Bad Bot Sophistication Levels 2021



Evasive Bad Bots	**65.6%**
Moderate	39.7%
Advanced	25.9%

No industry is immune to bad bots

Bad bots impacted all industries in 2021. Their ability to perform various malicious actions, often in a repetitive manner, makes them the ideal tool for executing tasks that would be tiresome for a human to do. Some bad bot use cases are shared across various industries, while others are industry-specific. Account Takeover fraud, as well as content and price scraping, are just a few examples of bot problems that are rampant across multiple industries, while scalping is mostly common on retail and ticketing websites.

Largest Share Of Bad Bot Traffic By Industry In 2021

1 Sports 57.1%	▲ 23.4%
2 Gaming & Gambling 53.9%	▲ 26.2%
3 Telecom & ISPs 46.9%	▲ 1.2%
3 Food & Beverages 44.6%	▲ 22.1%
5 Computing & IT 35.7%	▲ 5.4%

Largest Share Of Advanced Bad Bot Traffic By Industry In 2021

1 Travel 70.3%	▲ 10.6%
2 Retail 31.7%	▲ 18.2%
3 Automotive 24.3%	▲ 19.3%
4 Education 23.2%	▲ 20%
5 Law & Government 14.3%	▼ 1%

Mobile is the preferred disguise

Bad bots continue to mask themselves as popular web browsers, attempting to follow legitimate user browser patterns by making their requests appear as if they were generated by a legitimate user browsing the web, hoping to evade detection. In 2021, Chrome is the leading choice once more. As more people browse the web through mobile devices, the use of mobile browsers like Mobile Safari and Mobile Chrome increases, more bad bots use them as cover. We are also observing an increase in the percentage of attacks being launched from mobile ISPs. The percentage of bad bots deployed from AWS reduced from 10.8% in 2020 to 7.95% in 2021.

Bad bots report as mobile user agents (Mobile Safari, Mobile Chrome etc.)	**35.6%**
Bad bots launched from mobile ISPs	**27.2%**
Bad bots using Amazon ISP	**7.95%**

Global bad bot traffic trends

The United States was the most affected country by bad bot attacks, targeted by 43.1% of attacks.

Top 5 Most Attacked Countries

1 United States	43.1%
2 Australia	6.8%
3 United Kingdom	6.7%
3 China	5.2%
5 Brazil	3.3%

Account Takeover attacks are more prevalent than ever

Imperva recorded an increase in the prevalence and sophistication of Account Takeover (ATO) attacks in 2021. Known as the identity theft of the digital age, ATOs involve bad actors attempting to gain illegal access to user accounts belonging to someone else. This is usually achieved using brute force login techniques such as credential stuffing, credential cracking, or dictionary attacks. These attacks use bots to run a list of stolen credentials against a login page (credential stuffing) or perform mass guessing of weak passwords (e.g. credential cracking, dictionary).

If successful, the implications of an account takeover are extensive. For customers, a successful ATO can lock them out of their account, while fraudsters gain access to their sensitive information such as credit card data, account funds, health records, retail reward points, and more. For a business, they must handle the high costs associated with ATO including increased customer support costs, revenue loss, tarnished reputation, risk of non-compliance with data privacy regulations, and more.

Similarly, bad actors attempting to takeover employee accounts is a business risk. Using compromised employee credentials, attackers can access the organization's network and execute malware or exfiltrate sensitive data to orchestrate a much more elaborate attack on the business and the broader supply chain.

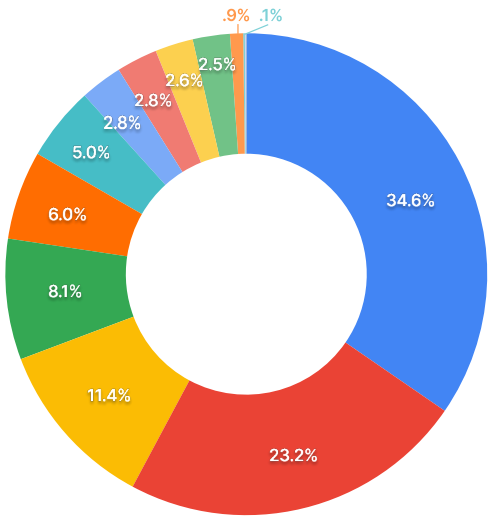
Account Takeover attacks by the numbers

148%	Increase in Account Takeover attacks between January and December 2021.
64.1%	Percentage of Account Takeover attacks making use of advance bad bots.
55%	Percentage of Account Takeover attacks that target the US.

Industries with the highest ATO ratio of all logins	Most targeted countries bt ATO attacks
Gaming & Gambling 34.9%	USA
Sports 34%	Singapore
Retail 18.1%	France
Travel 9.7%	Puerto Rico
Telecom & ISP 5.9%	Chile
Food & Beverage 5.4%	Germany

Most-attacked industries

The following chart illustrates what industries experienced the largest volume of Account Takeover attacks in 2021. Financial Services were targeted by just over a third of all ATO attacks (34.6%), followed by Travel (23.2%), Business Services (11.4%), and Retail (8.1%).



Account Takeover Attacks by Industry

Financial Services	34.6%
Travel	23.2%
Business Services	11.4%
Retail	8.1%
Entertainment & the Arts	6.0%
Telecom and ISPs	5.0%
Law & Government	2.8%
Gaming & Gambling	2.8%
Computing & IT	2.6%
Food & Beverage	2.5%
Sports	.9%
Education	.1%

Account Takeover attacks increased in H2

During the second half of 2021, Imperva Threat Research monitored an increase in ATO attacks. It started with a massive spike in attacks on Financial Services in June, which generated a 3,000%+ increase in malicious login traffic compared to the previous month. In October, attacks on Healthcare websites spiked (77%), coinciding with the general availability of the COVID-19 vaccine booster. At the end of the year, attacks on Gaming websites peaked (207% increase), coinciding with the holiday shopping season.

From online fraud to unfair advantage

Bad bots create trouble for security practitioners and others across an organization – from marketing to eCommerce and fraud teams. Most importantly, bots stand in the way of legitimate customers, and more concerningly, are a source of online fraud, including Account Takeover. Below are some of the ways bots have created disruptions for organizations and consumers during the past year.

Attacks are growing in frequency, intensity, and complexity

Over the past year, as investigated throughout this report, bot attacks became more prevalent than ever before, using advanced tools and techniques to break records for attack intensity. For example, in January 2022, Imperva Advanced Bot Protection detected and mitigated the largest bot attack in Imperva history. Over the course of four days, a web scraping attack targeted a global job listing website, pummeling it with no less than 400 million requests, originating from almost 400,000 unique IP addresses. The attacker used a large volume of IP addresses in an attempt to evade detection. With nearly 400,000 unique IP addresses at their disposal, each IP was making just 10 requests per hour, on average, with the intent of remaining below the rate-limit threshold of the site's bot defenses. For context, the traffic spike during the attack was 30x compared to regular traffic on this site.

Web scraping legality remains debatable

The last word has not yet been spoken in the legal battle between LinkedIn and hiQ Labs, which describes itself as a "data science company, informed by public data sources, applied to human capital". LinkedIn is attempting to stop hiQ from scraping personal information from users' public profiles. After the Ninth Circuit appellate court's decision in favor of allowing bots to scrape publicly available content, LinkedIn filed its petition requesting Supreme Court review in March 2020. Indeed, in June 2021, the Supreme Court provided LinkedIn with another chance to stop hiQ. The Supreme Court stated that it would not take on the case, however. Instead, it ordered the appeals court to hear the case again in light of its recent ruling, which found that a person cannot violate the Computer Fraud and Abuse Act (CFAA) if they improperly access data on a computer they have permission to use.[2] This isn't the only legal battle LinkedIn is currently fighting; in February 2022, LinkedIn filed a complaint against a group of Singapore-based data scrapers Mantheos Pte. Ltd., Jeremiah Tang, Yuxi Chew, and Stan Kosyakov. The complaint claims that they illegally profit from scraping data from LinkedIn's website, in violation of its terms of services and to its users' detriment.[3]

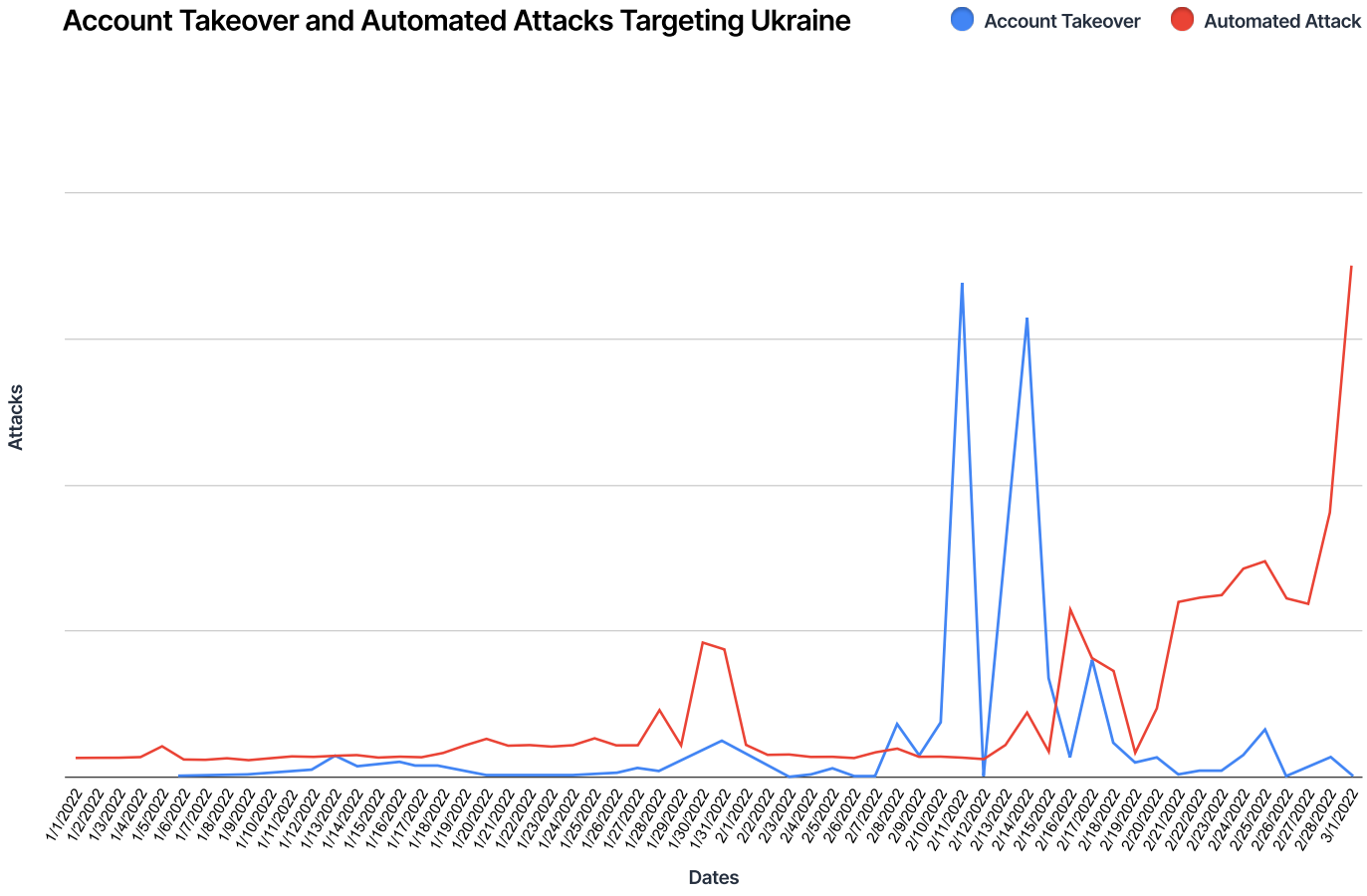
The Account Takeover (ATO) threat is bigger than ever

Of the many bot fraud use cases, ATO remains the most prevalent and perhaps most impactful. In the UK, ATO was the most common online fraud in 2021.[4] In the US, 22% of adults have been victims of Account Takeovers, which amounts to over 24 million households.[5] Social media and banking accounts were the most common accounts taken over. Imperva Threat Research recorded an increase of 148% in ATO attacks throughout 2021. 64.1% of these attacks made use of advanced bad bots, armed with the latest, most sophisticated evasion techniques. The US was targeted by 55% of attacks.

2. https://techcrunch.com/2021/06/14/supreme-court-revives-linkedin-bid-to-protect-user-data-from-web-scrapers/
3. https://lawstreetmedia.com/news/tech/linkedin-sues-singapore-based-data-scrapers/

Increased bot activity in Ukraine

Imperva Threat Research observed a 145% spike in automated attacks targeting Ukrainian web applications between February 24 and March 1, likely intended to disrupt services. The attacks recorded made use of advanced bots that facilitate distributed denial of service (DDoS) attacks, fraud, and malicious code injections. These attacks are usually aimed to deny critical services across financial, telecom, and energy. Additionally, Imperva recorded and stopped two massive ATO attacks on February 11 and 14.



4 https://www.moneymarketing.co.uk/news/action-fraud-initiates-110-investigations-into-online-frauds/
5 https://www.security.org/digital-safety/account-takeover-annual-report/

Appointment booking bots

Whenever there is high demand for a product or service, there is usually someone willing to pay a premium to "skip the virtual line." This creates a financial incentive for bad bot operators to attack. For example, Imperva mitigated such attempts from third-party providers attempting to scrape a driver's test booking domain to find available appointments for paying clients. Some of these spikes amounted to 15-20x the average traffic on the site. In a separate incident, malicious actors used bad bots to automatically book all available residency permits and visa appointments.[6] Cybercriminals then attempted to sell these appointment slots for upwards of €400.[7] The consequences of not being able to schedule such appointments are grave, preventing legitimate humans from being able to secure their visas, risking them living in the country illegally.

Scalpers flourish as an ongoing chip shortage persists

Some of the pandemic's ripple effects have triggered chain reactions that continue to cause problems, from supply-chain issues to the global shipping crisis and more. One particularly painful problem is the global chip shortage that is severely hampering production rates for many electronic devices. Wherever supply fails to meet demand in today's economy is fertile ground for scalpers. Just as Imperva recorded massive bot traffic around the release of the next generation gaming consoles and GPUs in 2020, a similar spike (though at a smaller scale) was recorded around the release of the Nintendo Switch OLED model in the second half of 2021. As the crisis stretches well into 2022, we predict that the situation will remain similar throughout the year. Retailers holding inventories of Playstation 5, Xbox Series X|S consoles, or GPUs must ensure that their online stores are adequately prepared to manage bot traffic and ensure a fair shopping experience for their customers.

OAT-005 SCALPING

Acquisition of goods or services using the application in a manner that a normal user would be unable to undertake manually.

Learn More

6 https://www.thelocal.fr/20220204/warning-over-bot-scammers-targeting-french-admin-appointments/
7 https://www.lemonde.fr/societe/article/2021/02/13/titres-de-sejour-le-trafic-lucratif-des-rendez-vous_6069858_3224.html

Can legal action be taken against scalpers?

The US Congress proposed the "Stopping Grinchbots Act of 2018[8]", a bill to prohibit the circumvention of control measures used by internet retailers to ensure equitable consumer access to products, and for other purposes. Last year, in the UK, a petition by Change.org was created, titled "Prevent/deter the buying and reselling of goods/services at inflated prices[9]". It garnered over 18,000 signatures and was given an official response by the UK Government on February 23, 2021: "The Government introduced legislation that prevents the use of automated software ('bots') to purchase event tickets which are sold on at an inflated price in 2018. We are discussing the issue of bulk purchasing of high demand items like graphics cards and games consoles through automated bots with trade associations such as Ukie, the trade association for the video games industry." In November 2021, Congressman Paul Tonko, representing New York's 20th Congressional District, joined by a group of congressional Democrats, announced a "Bill to Stop Cyber Grinches from Stealing Christmas". It is clear, then, that the matter is gaining traction, but the question still stands – are these attempts at taking legal action enough to deter scalpers? The answers remain unclear. What is clear, however, is that for the foreseeable future, the task of managing bad bots is in the hands of retailers. Online retailers must fend for themselves in the battle of keeping high-demand product launches free of unwanted bot traffic and fair for all legitimate consumers.

Bots enrolling in college

It would appear that no stone is being left unturned by bot operators when it comes to potential money-making opportunities. On March 11, 2021, the Higher Education Emergency Relief Fund III (HEERF III) was authorized and signed into law by the American Rescue Plan (ARP), Public Law 117-2, providing $39.6 billion in support to institutions of higher education to serve students and ensure learning continues during the COVID-19 pandemic. According to The Washington Post[10], the US Congress has provided a total of $76.2 billion for colleges and universities to pivot online, stave off steep financial losses, and help students weather the public health crisis. Significant portions of these federal emergency grants were provided to students to help with food, housing, course materials, technology, healthcare, and child care. In an attempt to take advantage of these COVID-19 related relief grants, an elaborate bot operation presumably enrolled fake students in active courses at various colleges. This type of online fraud is referred to by the OWASP as OAT-019 Account Creation. Several colleges have been investigating this potentially widespread fraud, involving fake "bot students," in what officials suspect is a scam to obtain financial aid or COVID-19 relief grants.

OAT-019 ACCOUNT CREATION

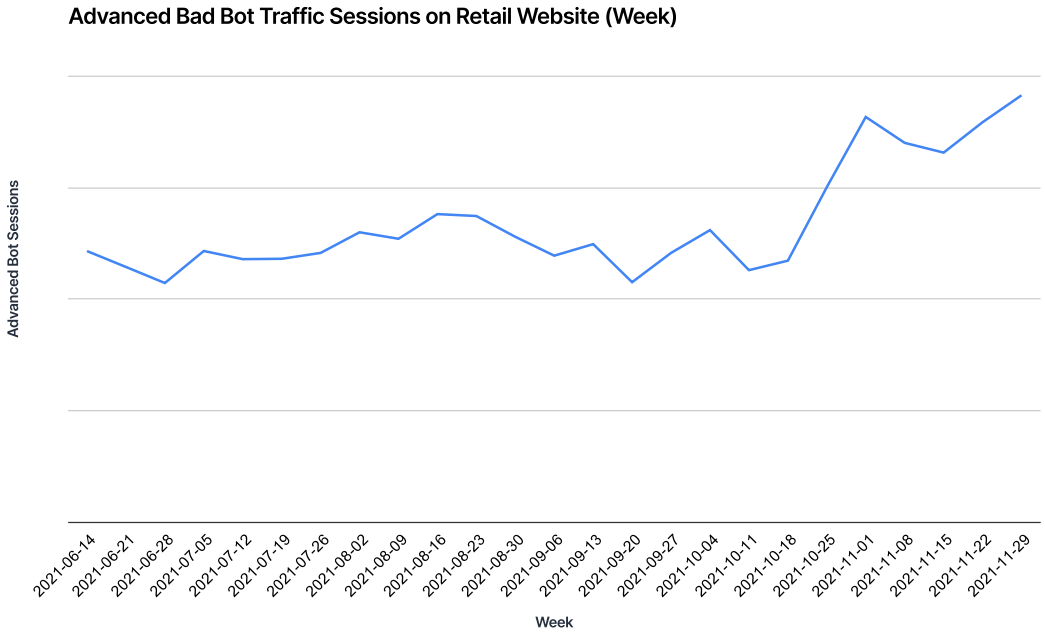
Bulk account creation, and sometimes profile population, by using the application's account sign-up processes. The accounts are subsequently misused for generating content spam, laundering cash and goods, spreading malware, affecting reputation, causing mischief, and skewing search engine optimisation (SEO), reviews and surveys.

Learn More

8. https://www.congress.gov/bill/115th-congress/house-bill/7160/text
9. https://petition.parliament.uk/petitions/561986
10. https://www.washingtonpost.com/education/2022/01/20/colleges-pandemic-aid-students-biden/

Holiday shopping season sees bot traffic hit a six-month high

Throughout 2021, eCommerce remained highly targeted by bad bots, with advanced bot traffic levels increasing by nearly 73% during November. During the week of Cyber Monday in 2021, Imperva Threat Research monitored a spike in bot traffic, growing 8% over the week of Thanksgiving and Black Friday. Of all the attacks monitored in November, 27% were carried out by advanced bots, compared to 23% in November 2020, indicating a clear pattern of increase in the volume and sophistication of bot traffic.



Hyped product drops remain a top-priority target

Targeting limited-edition product launches, or “online drops,” is a highly profitable income source for bad bot operators. Sneakers and concert tickets remain high-priority “drops” and were recently joined by gaming consoles and graphics cards. One trend of recent years is retailers’ decision to use Black Friday as the time frame for these highly sought-after product launches, making an already peak time for bot attacks from Grinchbots and others even more so. During the week of Black Friday 2021, Imperva recorded and mitigated a gigantic scalping attack on a global retailer’s drop of a limited-edition collectors’ item – an attack that consisted of no less than 9 million bot requests to the product page in a mere 15 minutes. For context, that’s 2,500% more than the average web traffic on the retailer’s site.

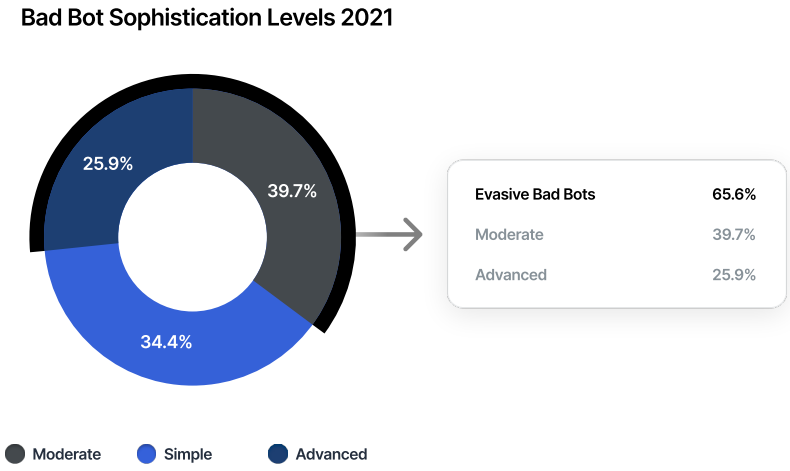
Account Takeover targets high-profile sporting events

As 2021 marked a year of a slow return to normal, Sporting events set to take place in 2020 were headed for a kickoff in the summer of 2021 – particularly the Euro 2020 tournament and the Tokyo Summer Olympic Games. Leading up to the Euro 2020 tournament, Imperva Threat Research monitored a 96% year-over-year increase in bot traffic on global sporting sites. In particular, UK gambling sites were heavily targeted by bot operators. Days that the English national team played were of particularly high risk, with ATO attacks spiking by two or three times the daily average compared to other days during the tournament. In the first week of the Summer Olympic Games, Imperva Threat Research monitored a spike in search engine impersonators. Traffic to sporting sites saw an abnormal 48% increase in Yahoo! impersonators, 66% increase in Baidu impersonators, and 88% increase in Google impersonators. During the second week of the Olympics, the volume of browser impersonators spiked by 103% above average. More concerning was the large increase in web traffic from IPs known to perform ATO attacks throughout Japan before and during the first week of the Summer Olympic Games. ATO attacks grew 43% ahead of the start of the Summer Olympic Games, spiking 74% during the first week of competition. The Tour de France was another event of interest last summer, with bot activity on sporting and gambling sites spiking 52% around the time it was set to start. That traffic was made up mainly of bot comment spammers, of which traffic increased 62%.

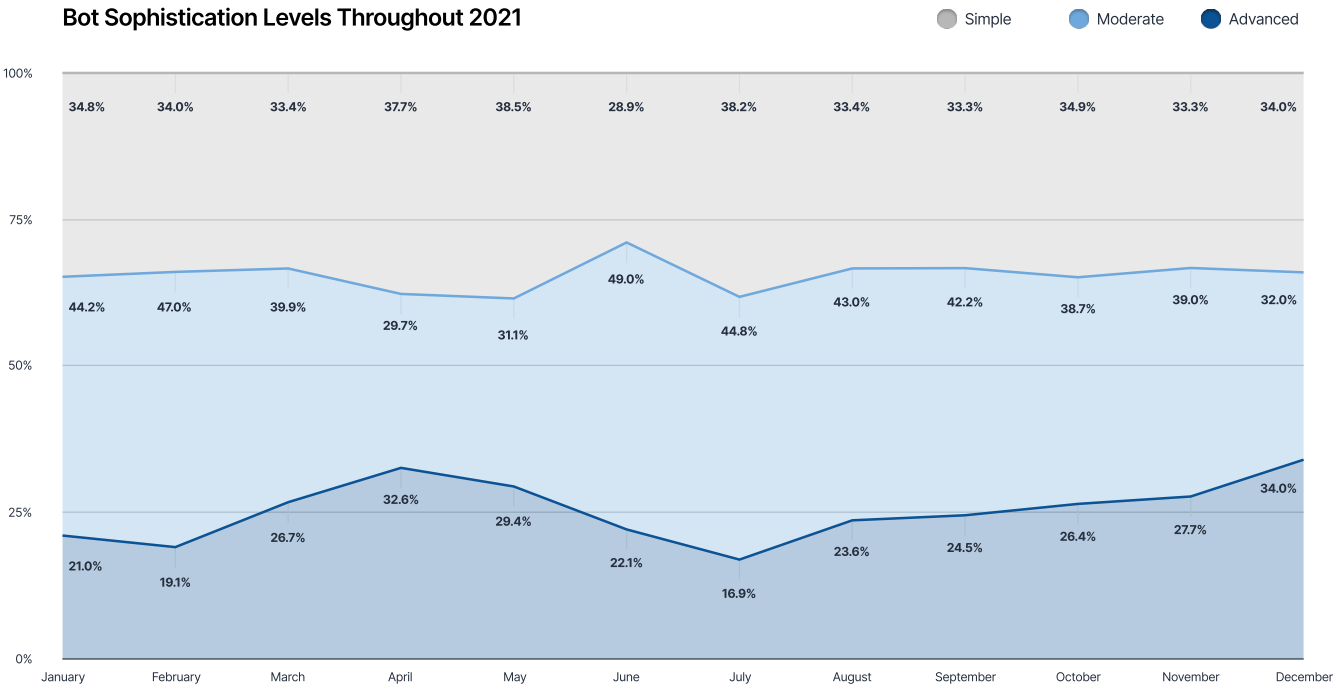
The bad bot landscape

Evasive bad bots are a major source of online fraud

This year, we see an increase in the sophistication level of bad bots compared to last year, with advanced bad bots accounting for 25.9% of all bad bot traffic in 2021, compared to 16.7% in 2020. Moderate bad bot levels remain similar, at 39.7% in 2021 compared to 40.4% in 2020. This year, advanced bad bot levels grew while the volume of simple bad bots declined. These changes influenced the development of Evasive bad bot levels, which made up a majority of bad bot traffic in 2021, accounting for 65.6% of all bad bot traffic. These are also the types of bots responsible for the majority of account takeover fraud. As more online fraud becomes reliant on automation, or bad bots, we will continue to see a rise in the sophistication level of these automated threats.



Breaking down bad bot sophistication levels in a monthly view reveals an upward trend in advanced bad bot traffic ratio in the second half of 2021, ending the year at record levels, accounting for 34% of all bad bot traffic in December.

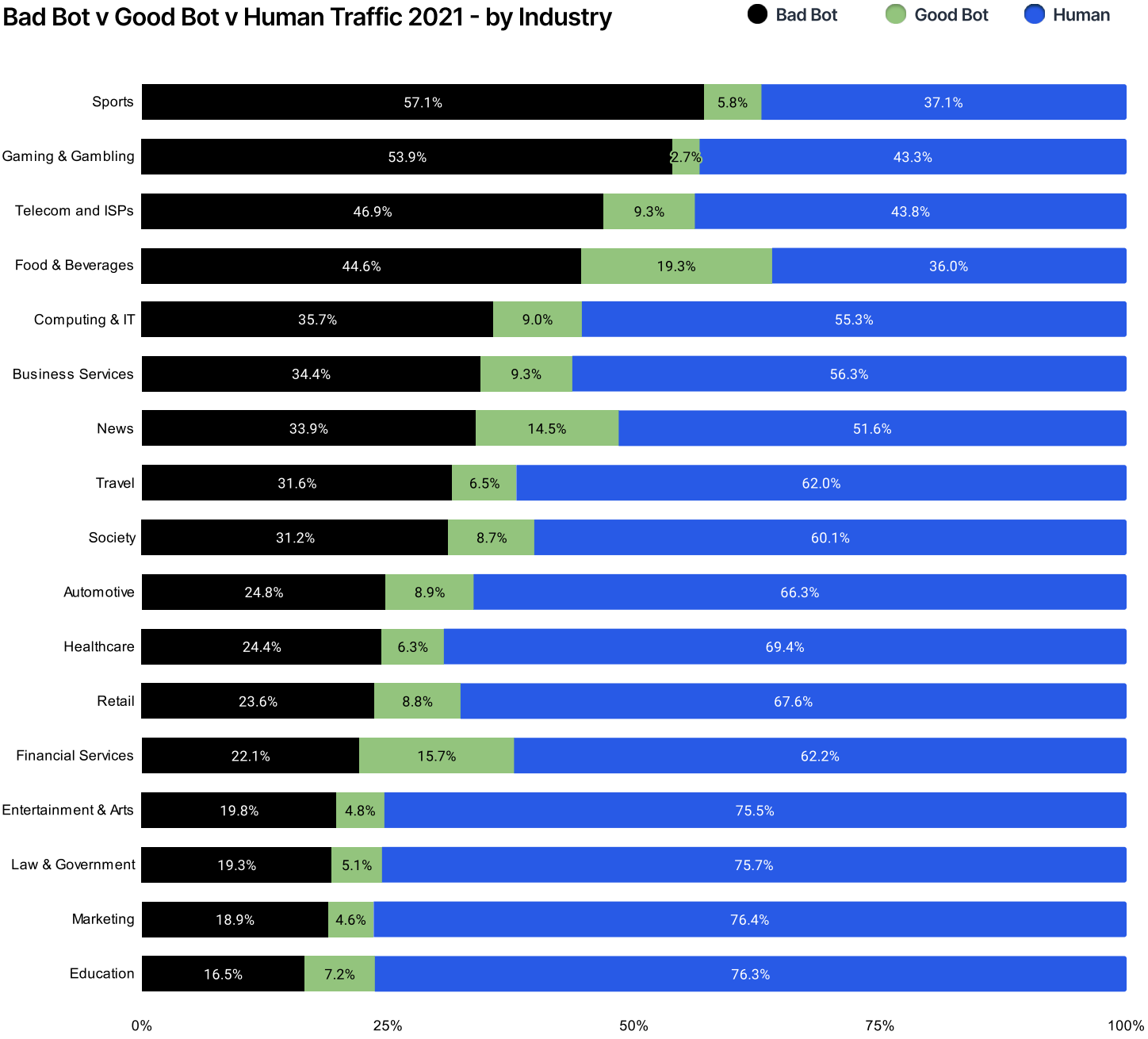


Bad bots by industry

Industry	What businesses are included?	What are bad bots doing?
Automotive	Manufacturers, dealerships, vehicle marketplaces	Price Scraping, Data Scraping, Inventory Checking
Business Services	Real estate, third party vendors like retail platforms, CRM systems, business metrics	Attacks on the API layer, Data Scraping, Account Takeover
Computing & IT	IT services, IT providers, services and technology providers	Account Takeover, Scraping
Education	Online learning platforms, schools, colleges, universities	Account Takeover for students and faculty, class availability, scraping proprietary research papers and data
Entertainment & Arts	Streaming services, ticketing platforms, production companies, venues	Account Takeover, Price Scraping, Inventory Checking, Scalping
Financial Services	Banking, insurance, investments, cryptocurrency	Account Takeover, Carding, Card Cracking, custom Content Scraping
Food & Beverages	Food delivery services, online grocery shopping, food & beverage brand sites	Credit Card Fraud, Gift Card Fraud, Account Takeover, Coupon Guessing
Gaming & Gambling	Online gaming, casinos, sports betting	Account Takeover, Odds Scraping, account creation for promotion abuse
Healthcare	Health services, pharmacies	Account Takeover, Content Scraping, Helpful bots, vaccine availability, Inventory Checking, vaccine appointment availability
Government	Law & government websites, citizen services, states, municipalities, metropolitans	Account Takeover, Data Scraping of business registrations listings, voter registration
Marketing	Marketing agencies, advertising agencies	Custom Content Scraping, ad fraud, denial of service, skewing
News	News sites, online magazines	Custom Content Scraping, ad fraud, comment spam
Retail	eCommerce, marketplaces, classifieds, lifestyle & fashion	Denial of inventory (Grinchbots, sneakerbots etc.), Credit Card Fraud, Gift Card Fraud, Account Takeover, Data and Price Scraping, skewing
Society	Nonprofits, faith and beliefs, romance and relationships, online communities, LGBTQ, genealogy	Data Scraping, Account Takeover, account creation, testing stolen credit cards on donation pages
Sports	Sports updates, news, live score services	Data Scraping (live scores, odds etc.)
Telecom & ISPs	Telecommunications providers, mobile ISPs, hosting providers	Account Takeover, competitive Price Scraping
Travel	Airlines, hotels, holiday booking	Price and Data Scraping, skewing of look-to-book ratio, denial of service, Price Scraping, Account Takeover

The following chart provides a breakdown of the traffic profile for each industry

Bad Bot v Good Bot v Human Traffic 2021 - by Industry



Sports

Sports websites had an astounding 57.1% of incoming traffic originate from bad bots in 2021. This is likely due to a series of high-profile, global sporting events like the Euro 2020 and the Tokyo Olympic Games taking place after a year of being postponed. As uncovered by Imperva Threat Research, bad bots heavily targeted sporting websites during these events, engaging in account takeover fraud, odds scraping, and comment spam.

Gaming & Gambling

Gaming & Gambling is a close second, with 53.9% of website traffic originating from bad bots. This category includes online gaming, casinos, and sports betting sites. Online fraud is highly prevalent in this industry – odds scraping, account takeover, and account creation are common threats in this industry.

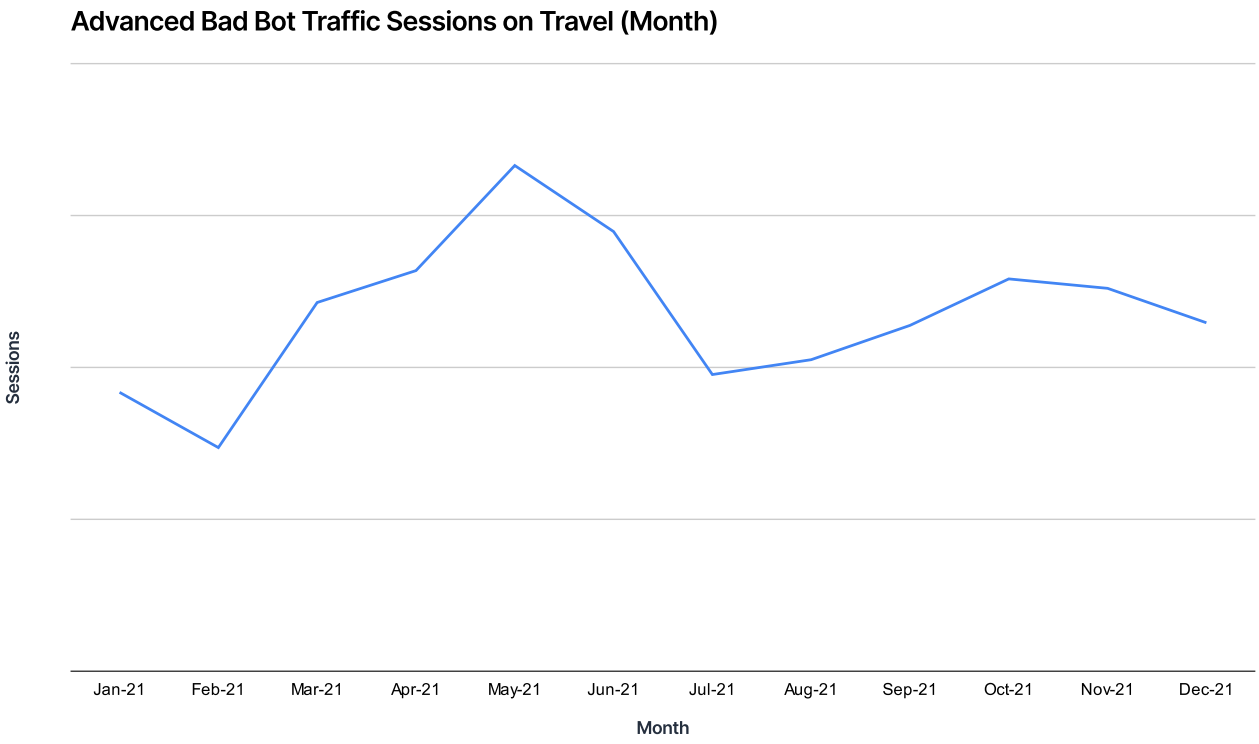
Telecom & ISPs

Telecom & ISPs websites had 46.9% of traffic originating from bad bots in 2021, a slight increase from 2020. This sector includes mobile ISPs, residential ISPs, hosting providers, and more. Account takeover for the payment methods saved within user accounts, as well as aggressive price and data scraping by competitors, are the main concerns for the industry.

Travel

Travel experienced sustained disruptions, related to the global pandemic, over the past two years. 31.6% of all web traffic to travel sites originated from bad bots in 2021. Considering the graph below, we can see the trend line of advanced bot traffic to the industry throughout the year. In early 2021, holiday bookings rose[11] in the hope that vaccines would bring an end to the pandemic. During that period, bad bot traffic to travel websites increased 126% between February and May. As news of the Delta variant emerged, holiday booking reservations were halted and bad bot traffic plunged 41% between May and July. This trend line underscores the reality that bots follow human behavior patterns. The travel industry suffers from the most complicated bot problems: Prices are scraped by direct competitors and third-party services in the expansive travel ecosystem. Unauthorized online travel agencies (OTAs), competitors, price aggregators, and metasearch sites use scraping bots to abuse the business logic of booking engines. Querying for any ticket they can sell, they skew look-to-book ratios, increase GDS transaction costs, and are responsible for site slowdowns and downtime — causing customer dissatisfaction during disruptions. Airlines specifically are suffering from ATO issues as bad bot operators attempt to get into user accounts and steal accumulated air mile balances.

11 https://www.theguardian.com/business/2021/jan/19/holiday-bookings-surge-as-covid-vaccinations-increase-travel-hopes



Food & Beverage

Food & Beverage websites had a significant portion of their traffic (44.6%) originating from bad bots in 2021. This category includes sites associated with food delivery services and online grocery stores. These sites are targets for Account Takeovers because criminals are after the various forms of payment available within customer accounts – stored credit card numbers, loyalty points, and gift card balances. In addition, account creation for promotion abuse is common. Price scraping by competitors is another common threat.

Retail

Retail websites had 23.6% of their traffic originating from bad bots in 2021. Scalping and denial of inventory are some of the most common automated threats plaguing online retailers. Price scraping by competitors and third parties, content scraping, Account Takeovers, credit card fraud, and gift card abuse are a few of the bad bot-related issues this industry is impacted by consistently.

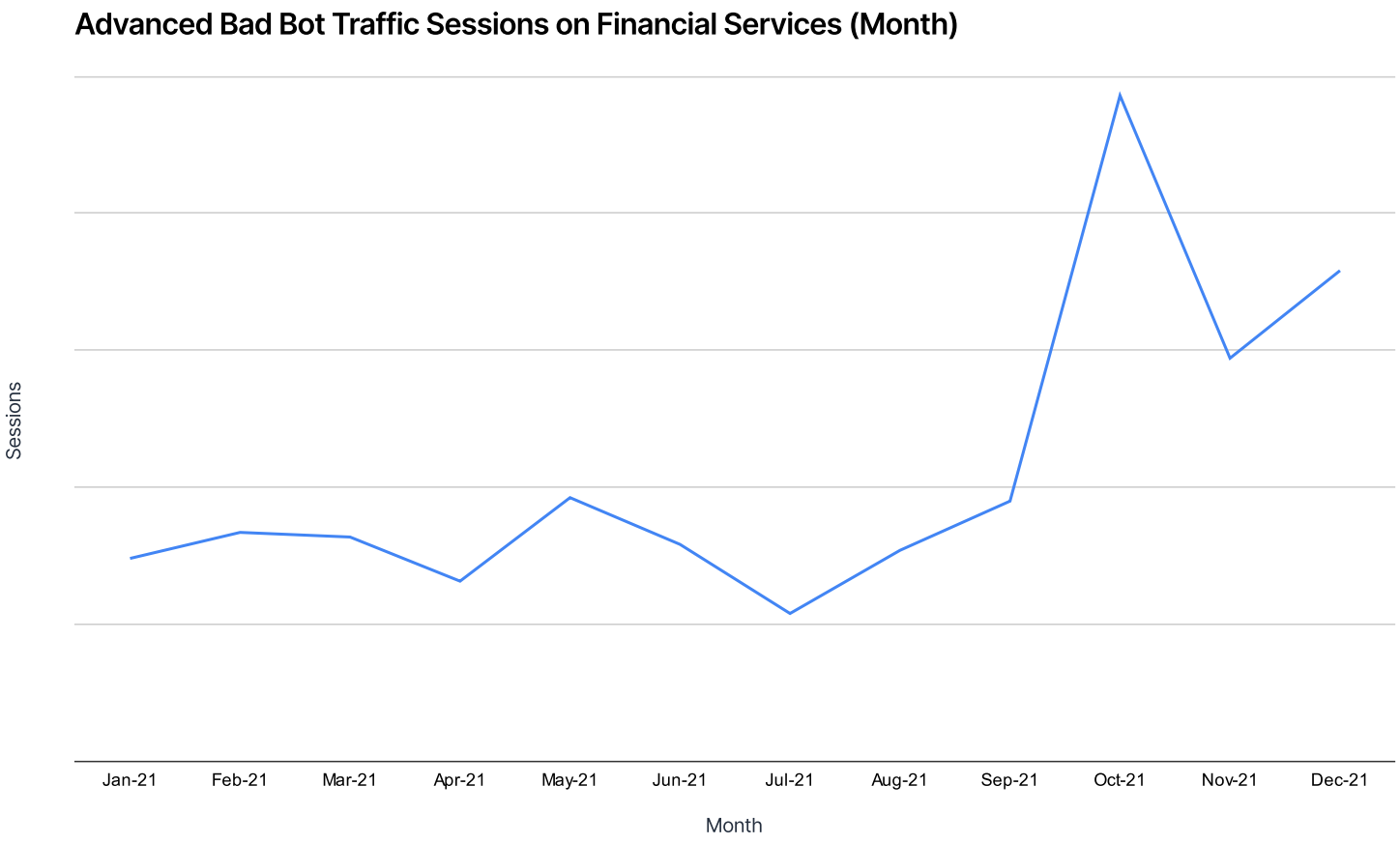
Healthcare

Healthcare had 24.4% of traffic originating from bad bots in 2021. Account Takeovers for sensitive health information is a common automated threat to this industry. In 2021, Imperva monitored a rise in “helpful bots” checking for vaccine availability or vaccine appointment availability. Imperva also recorded an increase in advanced bad bot traffic to healthcare websites that started in July 2021 and continue into 2022.

11 https://www.theguardian.com/business/2021/jan/19/holiday-bookings-surge-as-covid-vaccinations-increase-travel-hopes

Financial Services

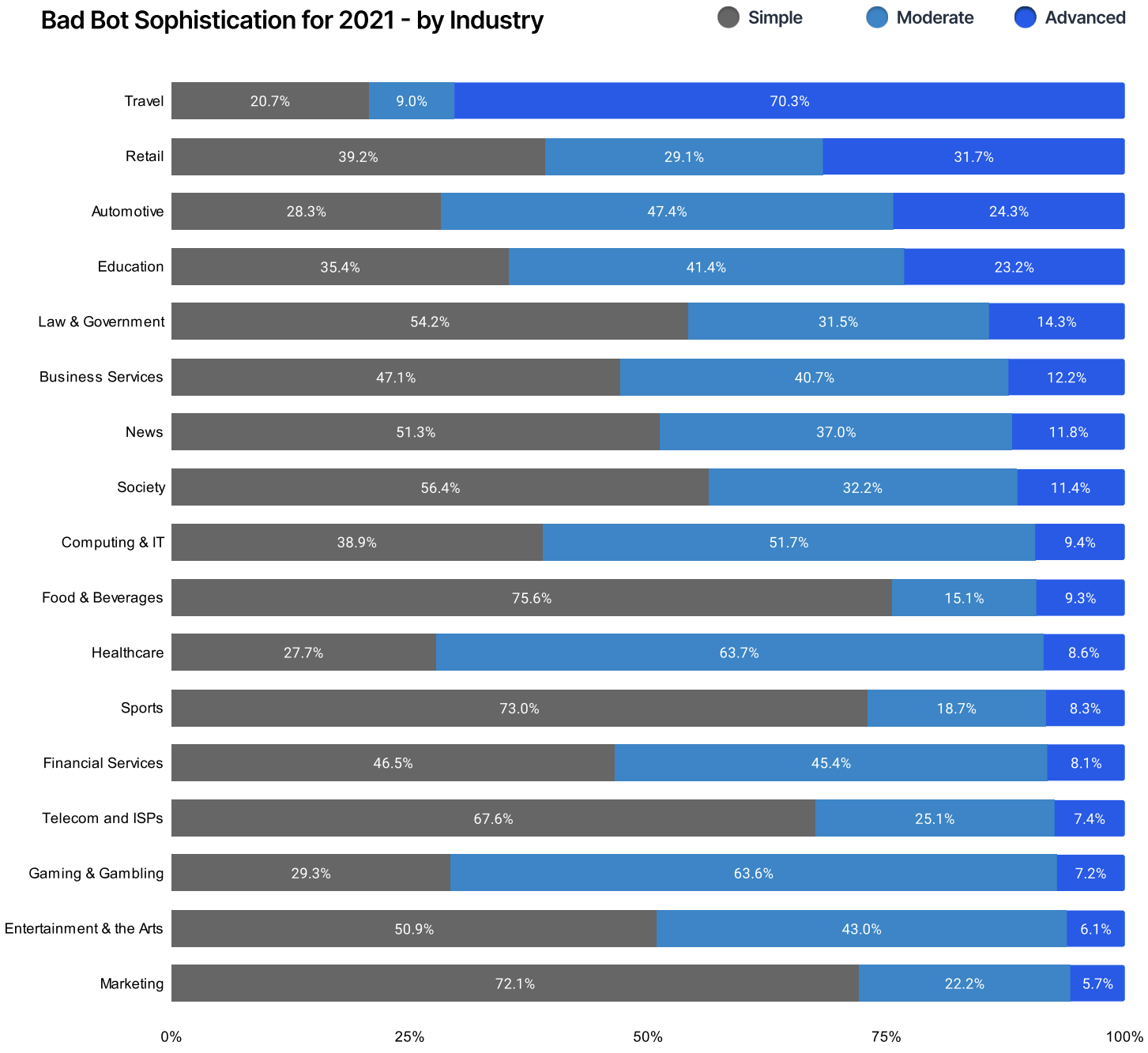
Financial Services had bad bots account for 22.1% of their website traffic in 2021. Organizations in this sector typically suffer from bad bots attempting to access user accounts using credential stuffing or credential cracking, credit card fraud, and custom content theft such as frequently changing interest rates. Imperva recorded a significant increase in advanced bad bot traffic to Financial Services websites during the last quarter of 2021, spiking 156% in October.



Bad bot sophistication by industry

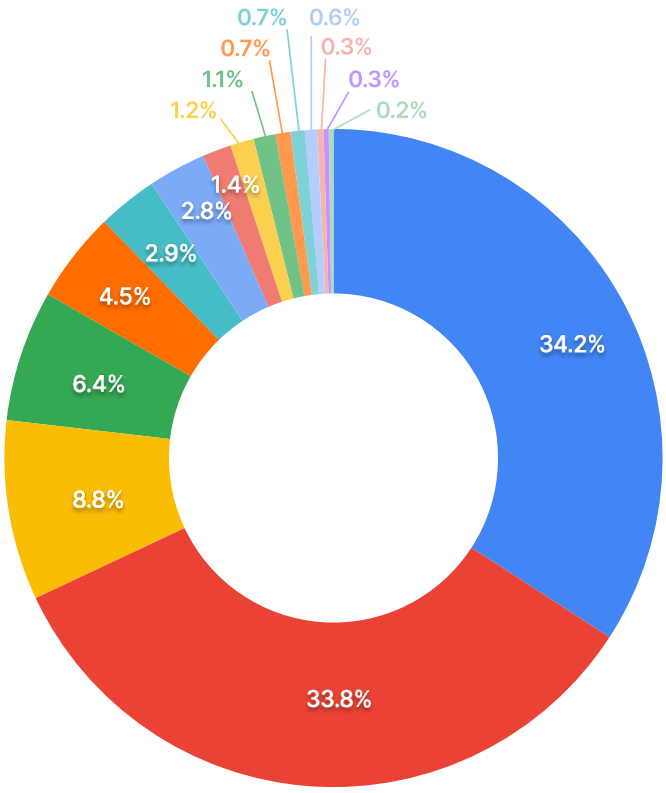
To better understand the bad bot risks each industry faced in 2021, Imperva Threat Research broke down bad bot traffic by sophistication levels. The larger the ratio of advanced bad bots, the more complex the bot problem risks are for the industry. In 2021, travel, retail, automotive, education, law and government, and business services experienced high proportions of sophisticated bad bot traffic throughout the year.

The level of sophistication doesn't necessarily correlate with the makeup of traffic. This means that an industry could have a high ratio of bad bot traffic, but they might all be classified as simple. It is important to note that any volume of advanced bot traffic should be considered a risk because advanced bad bots are able to achieve their goal while performing fewer requests than simpler bad bots.



Advanced bot attacks by industry

The distribution of advanced bot attacks across each industry provides a different perspective and reveals what industries were targeted the most. The top targets, travel, and retail, coincide with the high ratio of advanced bot traffic both industries experience. Alternatively, Financial Services sees a higher ratio of simple and moderate bots, but is still heavily targeted by advanced bots. This means that the ratio of advanced bad bots doesn't necessarily mean that the industry is targeted more often. This finding could imply that websites in this industry might have a higher number of bots classified as simple and moderate, which is still a threat to the business and its customers.



Most Targeted Industries by Advanced Bots in 2021

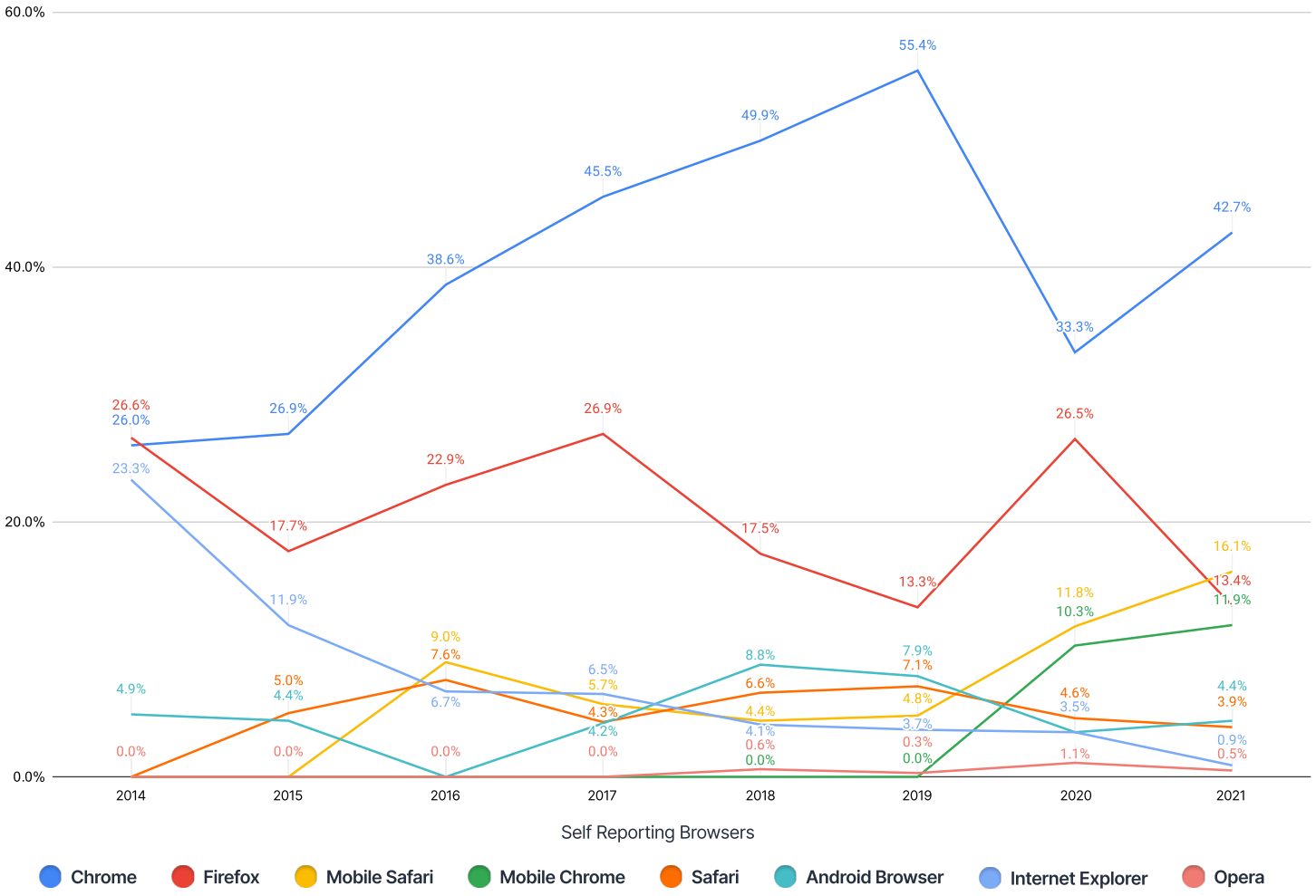
Travel	34.2%
Retail	33.8%
Financial Services	8.8%
Business Services	6.4%
Computing & IT	4.5%
Automotive	2.9%
Gaming & Gambling	2.8%
Healthcare	1.4%
Food & Beverage	1.2%
Society	1.1%
Education	0.7%
Law & Government	0.7%
Telecom & ISPs	0.6%
Sports	0.3%
Entertainment & Arts	0.3%
News	0.2%

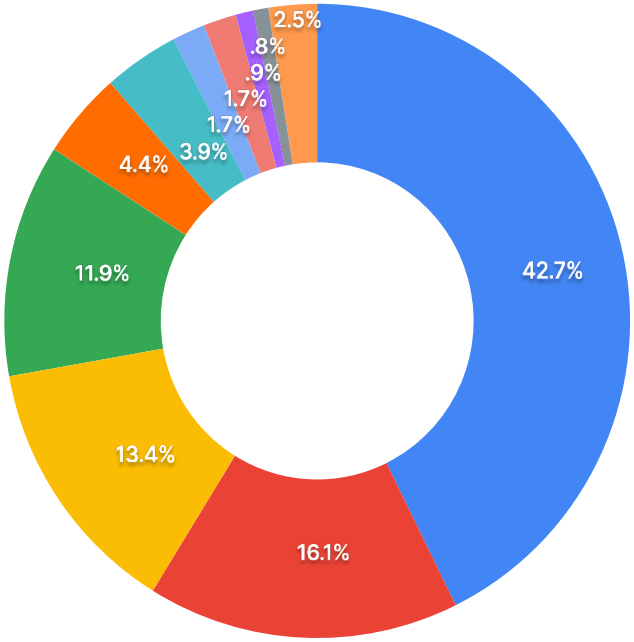
Bad bot identity: user privacy settings accelerate the shift to mobile

One of the many techniques bot operators use to avoid detection is to masquerade as legitimate users. They do so by reporting their user agent as a web browser or mobile device that is commonly used by legitimate human users.

This year, bots masquerading as Chrome browsers rose in volume after decreasing in 2020. This accounted for 42.7% of traffic in 2021, compared to 33.3% in 2020. The use of Mobile Chrome increased as well, amounting to 11.9% of traffic. Mobile Safari increased from 11.8% of traffic in 2020 to 16.1% in 2021, surpassing Firefox for the first time (13.4%). One reason for this increase could be the improved user privacy settings that this browser now offers, allowing bots to mask their behavior, making them even harder to detect.

Top Self Reporting Browsers by Bad Bots 2014-2021





Top Self Reporting Browsers by Bad Bots in 2021

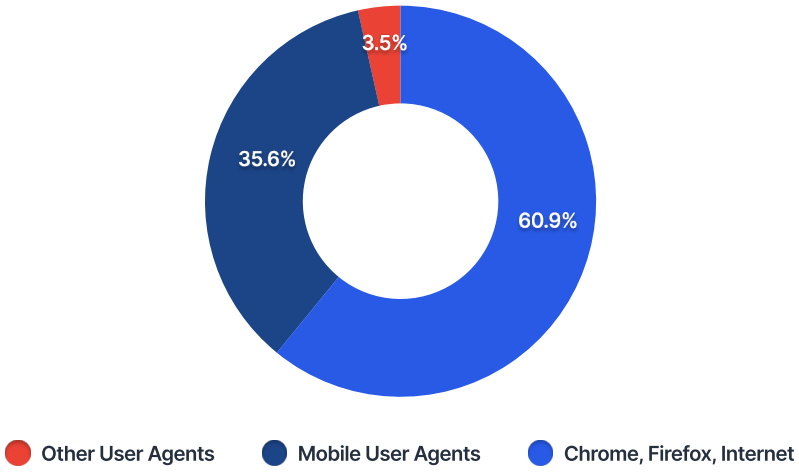
Chrome	42.7%
Mobile Safari	16.1%
Firefox	13.4%
Mobile Chrome	11.9%
Android Browser	4.4%
Safari	3.9%
Other	2.5%
Webkit Browser	1.7%
Samsung Browser	1.7%
Internet Explorer	0.9%
Google Search App	0.8%

Bad bots on the move: Mobile bots' popularity peaks

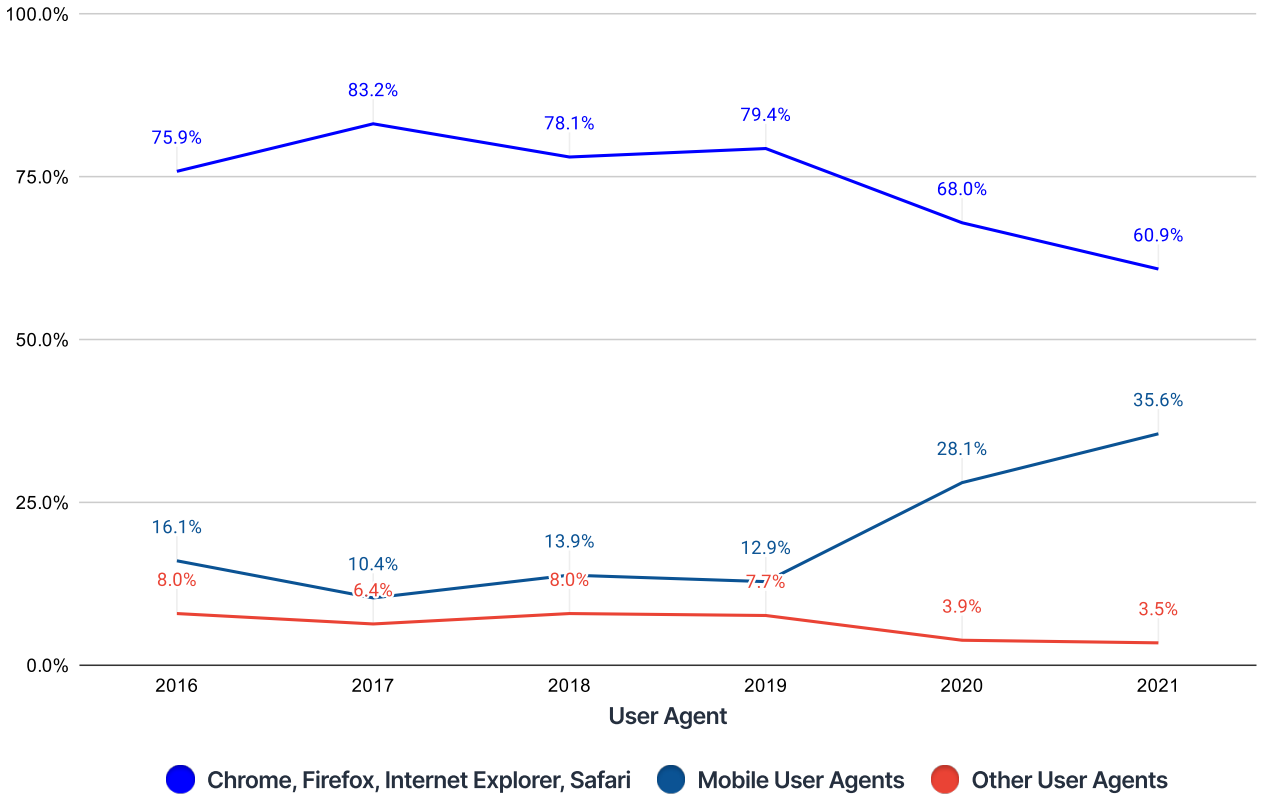
As the popularity of mobile browsing grows, bad bots are following the trend in their continued attempt to mimic human behavior and traffic patterns. In addition, the added privacy features for mobile Safari enable bad bots to better disguise themselves. While the majority of bad bots (60.9%) are self-reporting as either Chrome, Firefox, Safari, or Internet Explorer, their popularity as a user agent is decreasing. At 60.9% of traffic, it is lower than the previous year (68%).

Meanwhile, reported use of bad bot mobile user agents are increasing, (28.1% in 2020 to 35.6% in 2021), eclipsing a third of traffic! The rest of the bad bot traffic, 3.5%, is reported as other user agents (e.g. Google Search App or QQ and WeChat browsers).

Bad Bot Reported User Agent Types 2021



Bad Bot Reported User Agent Types 2016-2021

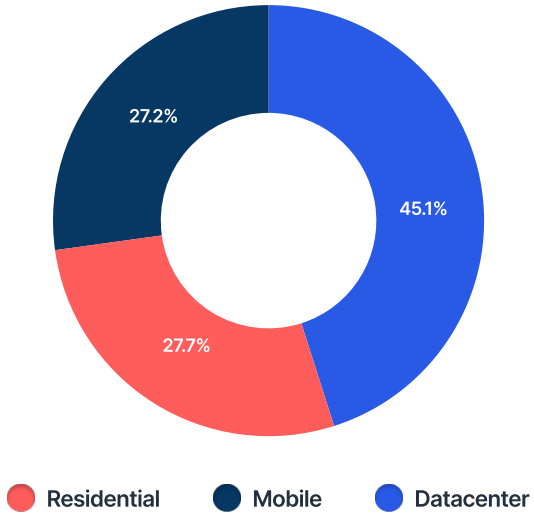


Mobile ISPs: A new bot favorite?

Data centers remain the origin for a majority of bad bot traffic (45.1%), yet preserving its downward trend from last year (54%). The amount of bad bots originating from residential ISPs decreased slightly, from 30.9% to 27.7%.

The popularity of mobile ISPs spiked in 2021, almost doubling the amount of traffic originating from them. They accounted for 27.2% of traffic compared to 15.1% in 2020.

Bad Bot Traffic by ISP Type 2021



The popularity of datacenters decreases

Bad bots were launched from 3,030 different ISPs in 2021.

- As more mobile ISPs are used to launch bad bot attacks, reliance on Amazon as an ISP is decreasing (10.8% in 2020 to 7.95% in 2021).
- Returning to the top, Digital Ocean and OVH SAS claimed the second and third spots with 2.24% and 2.10%, respectively.

Residential and mobile ISPs on the rise

As the residential and mobile ISP markets expand, attackers have more options to launch botnets from. Choosing a residential or mobile ISP allows them to masquerade as legitimate users. In 2021, 54.9% of bad bot traffic originated from residential and mobile ISPs. With more mobile ISPs now adding residential service and vice versa, we predict more bot attacks being launched from those.

Top 10 Bad Bot Originating ISPs 2021

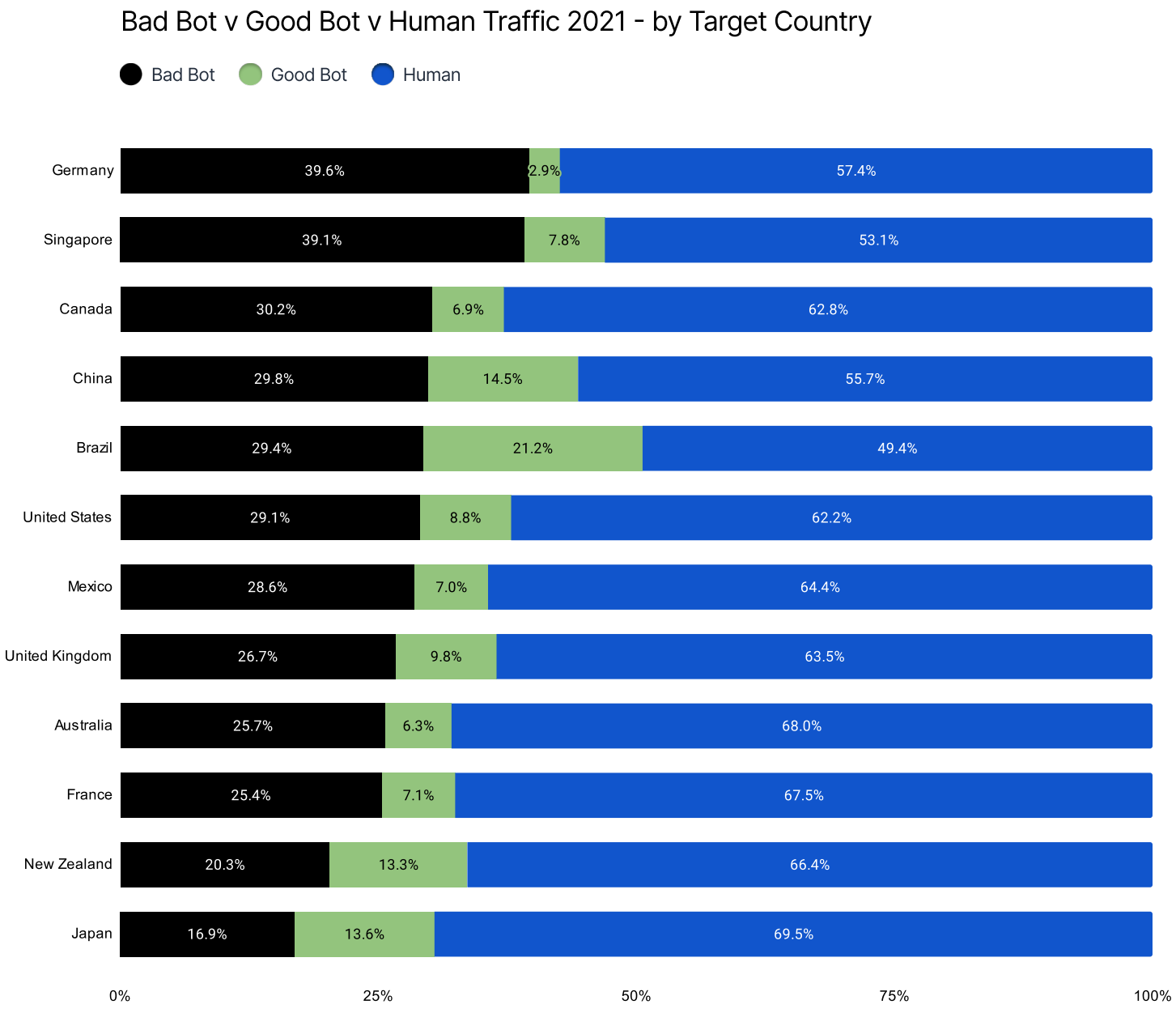
Rank	ISP	% of traffic
1	Amazon.com	8%
2	Digital Ocean	2.24%
3	OVH SAS	2.10%
4	WhiteLabelColo	2.07%
5	Comcast Cable	1.99%
6	Spectrum	1.88%
7	Contabo GmbH	1.84%
8	Corporacion Dana S.A.	1.81%
9	PT Telkom Indonesia	1.80%
10	Viettel Group	1.12%

Top 10 Bad Bot Originating ISPs 2021

Rank	ISP	% of traffic
1	Spectrum	1.88%
2	PT Telkom Indonesia	1.80
3	Viettel Group	1.12%
4	ER-Telecom	0.78%
5	Tigo Colombia	0.78
6	China Telecom	0.73%
7	CAT Telecom	0.55%
8	Turk Telekom	0.54
9	Telecom Argentina S.A.	0.52%
10	PT Mora Telematika Indonesia	0.50%

Bad bots by nation states

Analyzing the proportion of bad bot traffic by country reveals that several nations exceeded the global average of 27.7%. Germany and Singapore saw almost 40% of traffic originate from bad bots. The United States was also higher than the global average, with 29.1% bad bot traffic

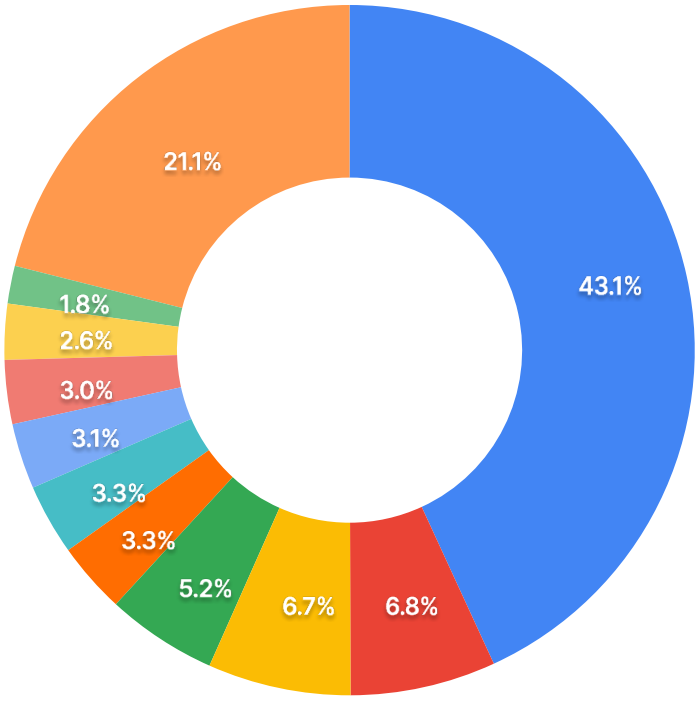


The United States and Australia were the most targeted countries

The United States was the leading target of bad bots in 2021 (43.1%), a slight increase over 2020 (37.2%). Australia was the second most attacked country by bad bots, targeted by 6.8% of all bad bot traffic. It was closely followed by the United Kingdom (6.7%) and China (5.2%).

Top 10 Most Attacked Countries by Bad Bots

1 United States
2 Australia
3 United Kingdom
4 China
5 Brazil
6 Germany
7 South Korea
8 Russia
9 Spain
10 Nigeria



Top Targeted Countries by Bad Bots 2021

USA	43.1%
Australia	6.8%
United Kingdom	6.7%
China	5.2%
Brazil	3.3%
Germany	3.3%
Korea	3.1%
Russia	3.0%
Spain	2.6%
Nigeria	1.8%
Other	21.1%

Recommendations

How should businesses protect themselves from bots and online fraud? Because every site is targeted for different reasons, and usually by different methods, there is no one-size-fits-all answer. But there are some proactive steps you can take to start addressing the problem today.

Security recommendations for detection of bad bot activity and automated fraud:

1. **Risk Identification:** Stopping bot traffic begins with identifying potential risks to your website
   Marketing and eCommerce campaigns bring more bots. For example - launching a limited quantity, high-demand product. Whether it is a highly sought-after pair of sneakers, a new generation gaming console, or a limited-edition collectors' item, announce a date and time for a coveted product launch and bots will be there to get their hands on it first. Make sure that you are prepared to handle the high volume of traffic that is going to include a high ratio of evasive bots trying to scoop up the products and deny your customers access.

   Understanding the ways your site could become a target is key to a successful bot management strategy. Some website functionalities are highly exploitable by bad bots. Adding login functionality creates the opportunity for Credential Stuffing and Credential Cracking attacks. Adding a checkout form increases the chances of credit card fraud (Carding/Card Cracking). Adding gift card functionality invites bots to commit fraud. Make sure that these pages have extra security measures and a more strict ruleset.

2. **Vulnerability Reduction:**
   Protect exposed APIs and mobile apps — not just your website — and share blocking information between systems. Protecting your website is only part of the solution; don't forget about the other paths that lead to your web applications and data.

3. **Threat Reduction: User-Agents:**
   Many of the bot tools and scripts contain user-agent strings with browser outdated versions. In contrast, humans are forced to auto-update their browsers to newer versions. Take steps to block outdated browser versions:

	Block End of Life more than 3 years	**Captcha** End of Life more than 2 years
Chrome version	<75	<85
Firefox version	<68	<78
Safari version	<12	<13
Internet Explorer version	<10	<11

4. **Threat Reduction: Proxies**

   Bad bots increasingly use proxy services to hide their attacks. Attackers do this to appear as human users by rotating bulk IP services in their requests. Not allowing access from bulk IP data centers will decrease the likelihood of botnet traffic. Examples of bot providers include Host Europe GMBH, Dedibox SAS, Digital Ocean, OVH SAS & Choopa, and LLC.

5. **Evaluate Traffic:**

   Evaluating traffic for bots can be difficult without clear signs or indications. Bot traffic can be associated with high bounce rates or low conversion rates. Another strong indication of bots is unexplained traffic spikes or high requests to a particular URL.

   Bots focusing on a specific event could explain the dramatic increase to a particular endpoint. Determine if there's a clear source from the increased traffic levels. Such examples can be seen in an IP, ISP, or URL receiving more than average traffic levels.

6. **Monitor Traffic:**

   On login pages, define your failed login attempt baseline, then monitor for anomalies or spikes. Set up alerts so you're automatically notified if any occur. Advanced "low and slow" attacks don't trigger user or session-level alerts, so be sure to set global thresholds.

   On checkout and gift card validation pages, an increase in failures, or even traffic, can be a signal of carding attacks or that bots such as GiftGhostBot are attempting to steal gift card balances.

7. **Awareness:**

   Stay aware of data breaches and leaks occurring around the world. The ease of buying credential dumps from breaches and renting bot infrastructure to automate an attack has made this a very real risk. Bots will often use newly compromised credentials for stuffing attacks and ATO, as they are more likely to still be active, increasing the probability of compromising user accounts on your site.

8. **Evaluate Bot Protection solutions:**

   In early bot attack days, you could protect your site with a few tweaks and configurations to block bad bots. The data explored throughout this report shows that these days are long gone. Today's bad actors are using bots for their ease of use and effectiveness. The tools used are constantly evolving, bot traffic patterns are difficult to detect, and their sources can shift frequently. In advanced bots, we are seeing attacks mimicking human behavior like never before. For these reasons, hackers widely choose bots to target your site, as their incentives are high with low risk. Today, it's almost impossible to keep up with all of the threats on your own. Your defenses need to evolve as fast as the threats, and to do that you need dedicated support from a team of experts.

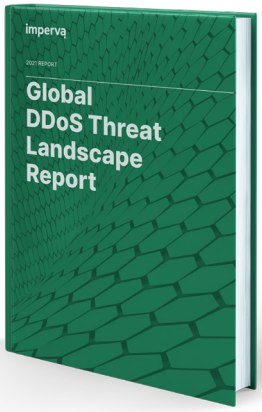
Imperva Threat Research

Global DDoS Threat Landscape

Key Findings

Over a half (5.7%) of all attacks recorded on retail websites in 2021 were carried out by bots.

Learn More



The State of Security within eCommerce 2021

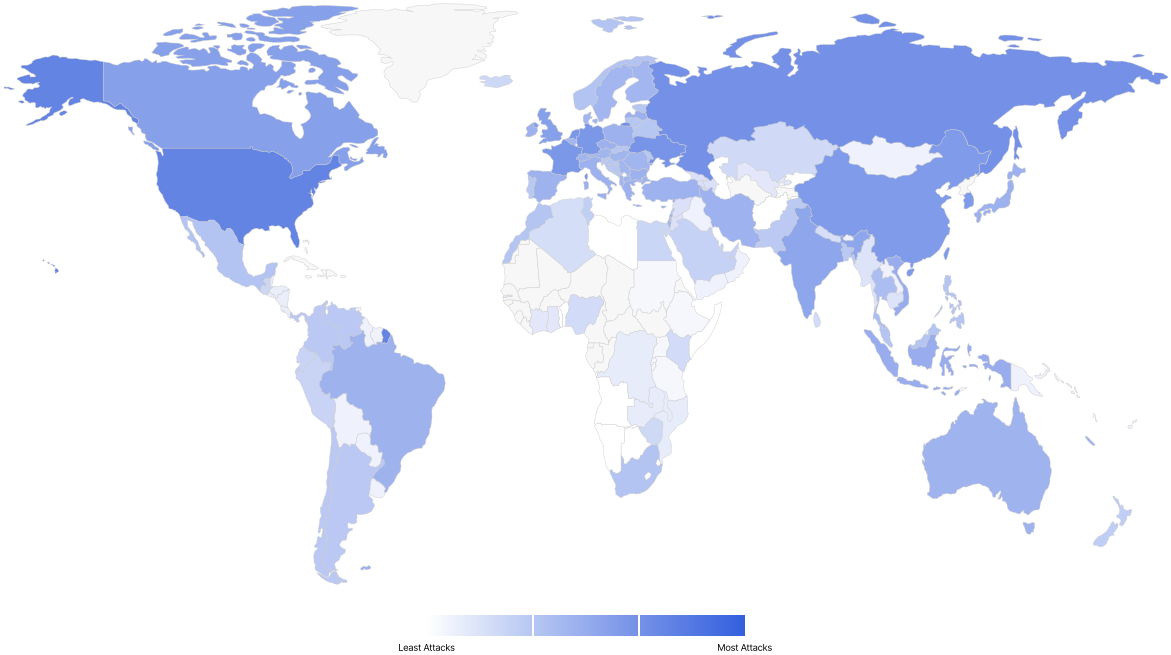
Key Findings

Over a half (5.7%) of all attacks recorded on retail websites in 2021 were carried out by bots.

Learn More

Cyber Threat Index

The Cyber Threat Index is a monthly measurement and analysis of the global cyber threat landscape. It provides an easy-to-understand score to track cyber threat levels consistently over time, as well as observe trends.



About Imperva Application Security

Imperva is the comprehensive digital security leader on a mission to help organizations protect their data and all paths to it. Only Imperva protects all digital experiences, from business logic to APIs, microservices, and the data layer, and from vulnerable, legacy environments to cloud-first organizations. Customers around the world trust Imperva to protect their applications, data, and websites from cyber attacks. With an integrated approach combining edge, application security, and data security, Imperva protects companies ranging from cloud-native start-ups to global multinationals with hybrid infrastructure. Imperva Threat Research and our global intelligence community keep Imperva ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into our solutions.

The Imperva Application Security combines best-of-breed solutions that bring defense-in-depth to protect your applications wherever they live — in the cloud, on-premises, or in a hybrid configuration:

- Web Application Firewall (WAF) solutions, which block the most critical web application security risks.
- DDoS protection with a 3-second mitigation SLA.
- API Security that integrates with leading API management vendors.
- Advanced Bot Protection for defense against all OWASP automated threats and online fraud.
- Runtime Application Self-Protection (RASP) for security by default against known and zero-day vulnerabilities.
- Client-Side Protection for discovery and monitoring of third-party services on sites or applications and defense against digital skimming, supply chain attacks, and Magecart.
- Developer-friendly Content Delivery Network (CDN) for the utmost performance.

Start your Application Security Free Trial today to start protecting your applications from bad bots and online fraud.