imperva

a Thales company

2024

Bad Bot
Report

2024
Bad Bot Report

Table of Contents

The 11th annual edition of the Imperva Bad Bot Report examines and investigates the nature of automated internet traffic, mainly automated bot attacks.

Such attacks are getting more sophisticated by the day, bypassing traditional detection methods and causing chaos on the internet. The report analyzes data collected from the Imperva global network in 2023, including nearly 6 trillion blocked bad bot requests anonymized across thousands of domains and industries.

This report aims to provide meaningful information about the nature and impact of bots to help organizations better understand the potential risks of bot traffic when not adequately managed.

The report focuses on bad bot activity at the OSI model's application layer (layer 7). These bot use cases are entirely different from volumetric DDoS attacks, which manipulate lower-level network protocols.

Bad bots interact with applications in a way that mimics legitimate users, making them more challenging to detect and block. They exploit business logic by exploiting an application's intended functionality and processes rather than its technical vulnerabilities. Bad bots facilitate high-speed abuse, misuse, and attacks on websites, mobile apps, and APIs. They allow bot operators, attackers, unsavory competitors, and fraudsters to engage in malicious activities.

Activities such as web scraping, competitive data mining, personal and financial data harvesting, brute-force login attempts, scalping, digital ad fraud, denial-of-service attacks, spamming, transaction fraud, and other similar activities can harm a business. These activities consume bandwidth, slow down servers, and steal sensitive data, leading to financial losses and damage to a company's reputation.

Before diving deep into the data,
let's define key terms we will use
extensively throughout this report.

What is a Bot?

In the context of the internet, a bot is a software application that runs automated tasks. Such tasks can range from simple actions like filling out a form to more complex functions like scraping a website for data.

What is a Bad Bot?

Bad bots are software applications that perform automated tasks with malicious intent. These bots can extract data from websites without permission to reuse it and gain a competitive advantage. They are often used for scalping, which involves obtaining limited availability items and reselling it at a higher price. Bad bots can also be used to create distributed denial-of-service (DDoS) attacks targeted at the application. Some bad bots undertake criminal activities such as fraud and outright theft. One example is bots that perform credential stuffing, one of the most prominent types of bot attacks. The Open Web Application Security Project (OWASP) provides a comprehensive list of 21 bot attacks in its Automated Threat Handbook[1].

What is the Difference Between Good and Bad Bots?

Not all bots found on the internet are bad. There are also good bots that serve valuable functions. For instance, some bots index websites for search engines or monitor website performance. Googlebot and Bingbot are examples of search engine crawlers that help create and maintain a searchable index of web pages. By indexing web pages, these bots help people find the most relevant sets of websites that match their queries. Such bots are essential for online businesses, allowing potential customers to easily find and access their websites, products, and services.

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

Even Good Bots can be a Cause for Concern

Good bots can significantly impact web analytics reports, as they can make certain pages appear more popular than they are. For instance, a good bot might generate an impression for a page on your website that you advertise, but that ad click never leads to the sales funnel. This can result in lower performance for advertisers and lead to skewed marketing analytics, ultimately leading to incorrect decision-making. Therefore, it is crucial to accurately distinguish between traffic generated by legitimate human users, good, and bad bots, to make informed business decisions.

Bad Bot Classification

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. This bot 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
The most sophisticated of bots emulates human user behavior like mouse movements and clicks to spoof bot detection. They use browser automation software, or malware installed within real browsers, to connect to sites.

Evasive
Sophisticated bot operators are very determined and persistent. If a bot management solution blocks them today, they will likely figure out why they were stopped and return tomorrow with a new technique to evade detection. These actors are using advanced bad bots, which are becoming more challenging to detect due to the advancements in evasion techniques. They often employ various techniques shared between Moderate and Advanced bad bots. Therefore, we group Moderate and Advanced bots to provide a fresh perspective on bad bot traffic analysis.

Evasive bots use complex tactics like cycling through random IPs, entering via anonymous proxies, using residential proxies, changing their identities, mimicking human behavior, delaying requests, and defeating CAPTCHA challenges. They use a "low and slow" approach to avoid detection and carry out significant attacks using fewer requests. This method reduces the "noise" generated by many bad bot campaigns, making it difficult to detect them.

Bad Bot Traffic Levels Continue to Rise

Bad bot traffic levels rose for the fifth consecutive year, indicating an alarming trend. This increase is partly driven by the increasing popularity of Artificial Intelligence (AI) and Large Learning Models (LLMs). In 2023, bad bots accounted for **32%** of all internet traffic – a **1.8%** increase from 2022. The portion of good bot traffic also increased, albeit slightly less significantly, from **17.3%** of all intent traffic in 2022 to **17.6%** in 2023. Combined, **49.6%** of all internet traffic in 2023 wasn't human, as human traffic levels decreased to **50.4%** of all traffic.

Bad Bot v Good Bot v Human Traffic 2023

32% Bad Bot **17.6%** Good Bot **50.4%** Human

Percentage change from the previous year

Bad Bots	**32%**	+1.8%
Good Bots	**17.6%**	+0.3%
Human	**50.4%**	-2.2%

Monthly Bad Bot Traffic Levels

The chart below displays a monthly trend analysis of the internet traffic profile. Interestingly, automated traffic surpassed human traffic in four different months throughout the year. The increase in bad bot traffic in December **(34.2%)** could be attributed to the increased number of attacks we recorded that month and slightly less human activity during the holiday season.

Bad Bot v Good Bot v Human Traffic Trend Over Month 2023

Bad Bot
Good Bot
Human

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Human	52.4%	51.5%	50.6%	48.5%	50.7%	49.8%	49.2%	49.2%	50.0%	50.2%	51.0%	50.8%
Good Bot	17.5%	17.7%	17.9%	18.6%	18.5%	19.3%	19.1%	18.9%	18.3%	17.1%	16.3%	15.0%
Bad Bot	30.1%	30.8%	31.6%	32.8%	30.8%	30.9%	31.7%	31.9%	31.7%	32.7%	32.7%	34.2%
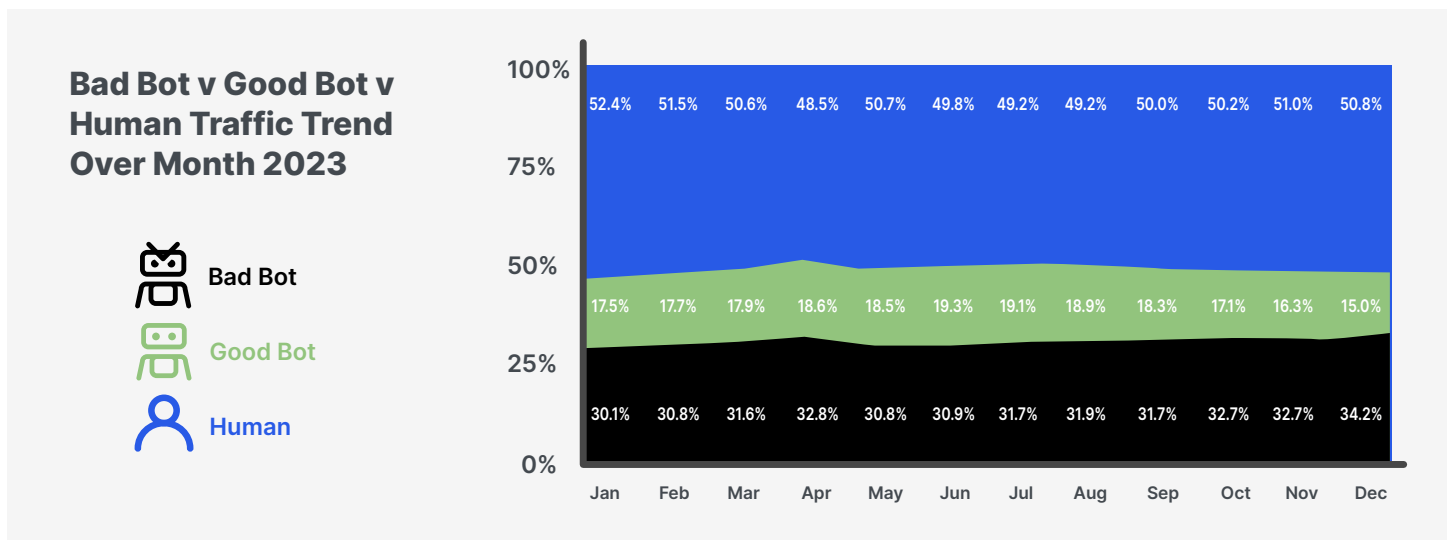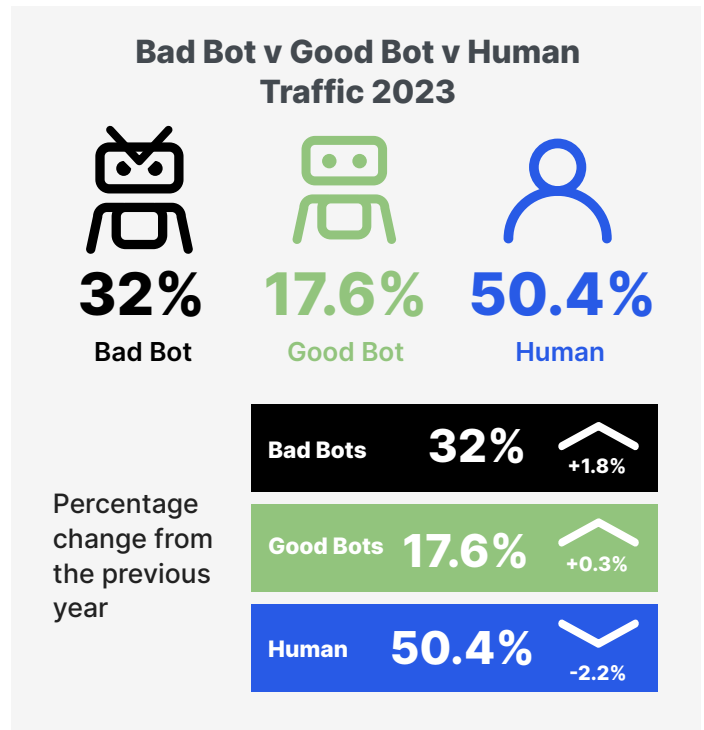
Bad Bot Traffic Over the Years

Imperva has been leading the fight against bad bots for over a decade. The chart below shows the good and bad bot and human traffic trends over the past 11 years.

In 2013, internet traffic comprised **23.6%** bad bots, **19.4%** good bots, and **57%** human traffic. Notably, 2014 witnessed a substantial increase in good bot traffic, rising from **20.98%** to **36.32%**, possibly influenced by more aggressive indexing by search engines. 2015 marked a decline in bad bot traffic to its lowest point as human traffic reached **54.4%**, attributed to a surge in new users, particularly from China, India, and Indonesia. 2016 and 2018 also saw lower bad bot activity, at **19.9%** and **20.4%**, respectively. However, from 2019 to 2023, bad bot traffic steadily increased, reaching **32.0%** of total internet traffic in 2023 – the highest ever.

Bad Bot v Good Bot v Human Traffic Trend 2013-2023

Bad Bot

Good Bot

Human

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Human	57.0%	40.9%	54.4%	61.3%	57.8%	62.1%	62.8%	59.2%	57.7%	52.6%	50.4%
Good Bot	19.4%	36.3%	27.0%	18.8%	20.4%	17.5%	13.1%	15.2%	14.6%	17.3%	17.6%
Bad Bot	23.6%	22.8%	18.6%	19.9%	21.8%	20.4%	24.1%	25.6%	27.7%	30.2%	32.0%
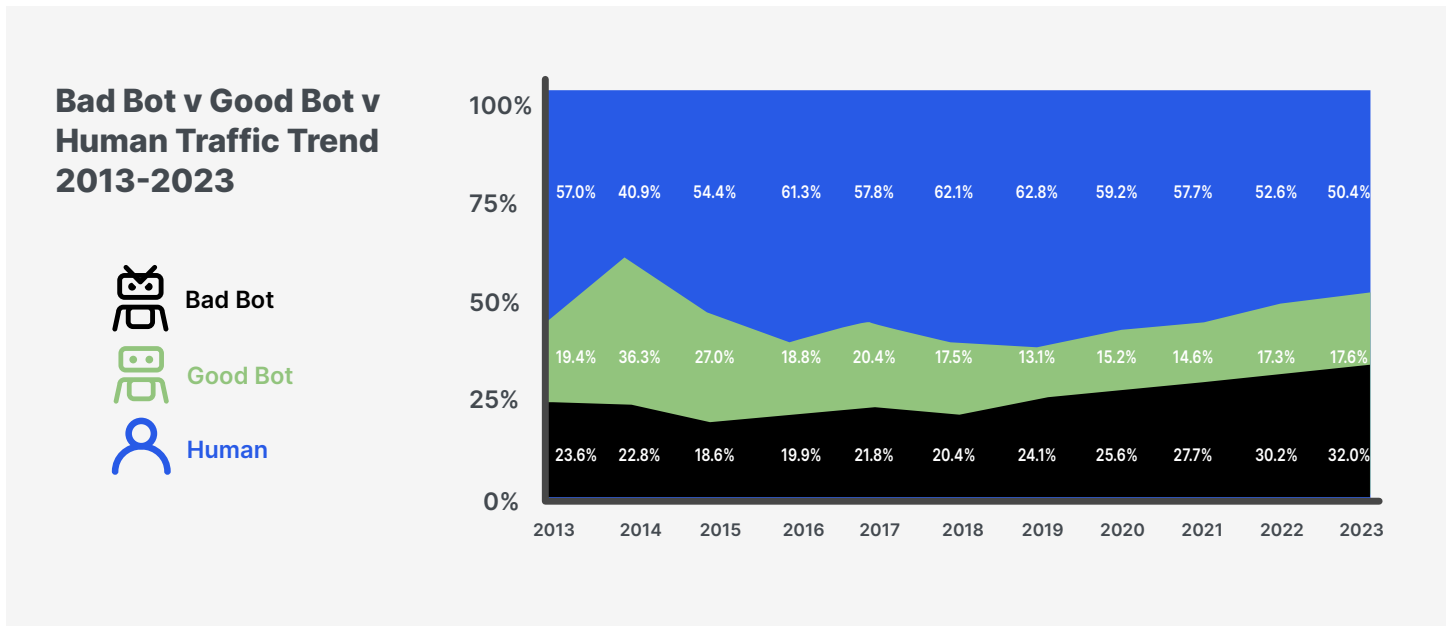
OWASP Automated Threats Account for Almost a Third of All Attacks
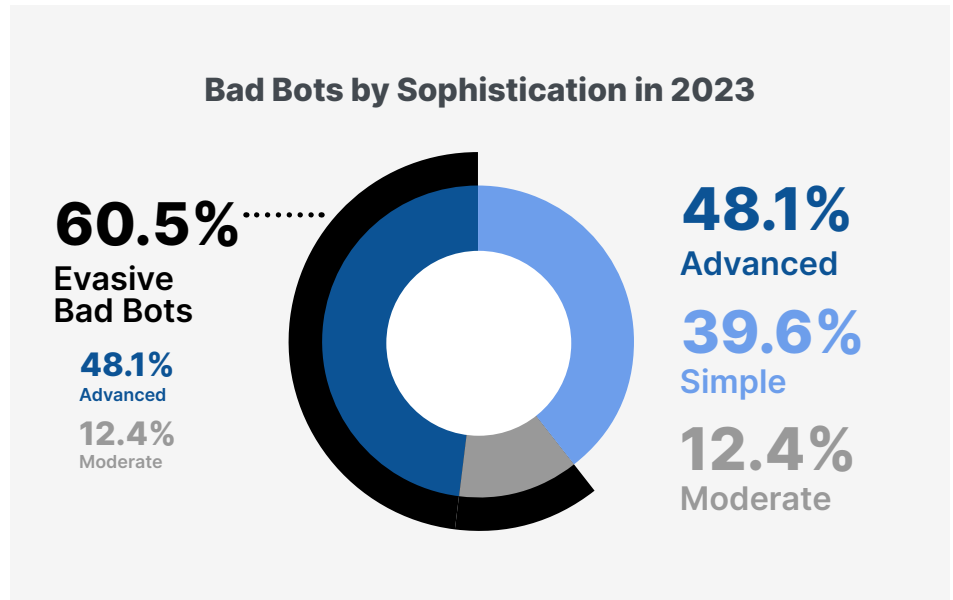
Of all the attacks recorded and mitigated by Imperva in the past year, 31.7% were automated threats, as defined by the OWASP. A drill down into the attack types reveals that **25%** of attacks mitigated were sophisticated bad bots that sought to abuse business logic.

Attacks Mitigated in 2023 by Category

55.9% OWASP WAF/API

12.4% DDoS

31.7% OWASP Automated
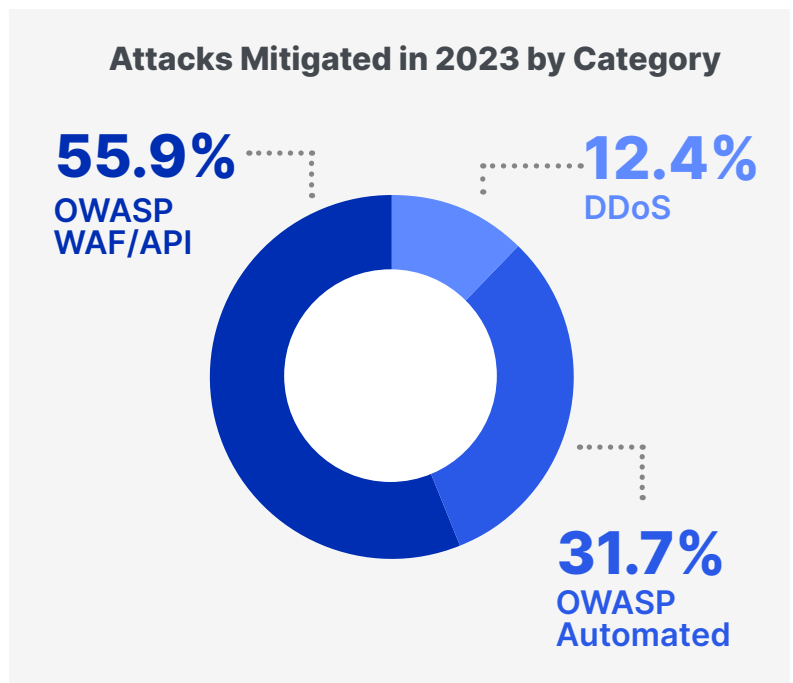
Are Moderately Sophisticated Bad Bots Going Extinct?

The growing adoption of AI technology affects the volume of bad bots on the internet and their level of sophistication. It created a distinct division between sophisticated actors with the means and resources to deploy advanced malicious bots and those who rely on basic tools, such as querying AI, to generate a bot script. The result? We're seeing an increase in simple bad bots, which accounted for **39.6%** of bad bot traffic in 2023, compared to **33.4%** in 2022 and up from **26.3%** five years ago. A second interesting trend is that the popularity of moderately sophisticated bad bots decreased, going from **15.3%** in 2022 to **12.4%** in 2023. If this trend continues, we may witness a gradual decline in the prevalence of this particular type of bot.

Advanced bots have gone from **51.2%** of bad bot traffic in 2022 to **48.1%** in 2023. These changes put evasive bad bots (the combination of moderate and advanced bot traffic levels) at **60.5%** of all bad bot traffic. This is a decrease from the previous year **(66.6%)**. Bad bot traffic remains highly sophisticated, with new advancements occurring by the day and emerging evasion techniques introduced.

Bad Bots by Sophistication in 2023

60.5%
Evasive
Bad Bots

48.1%
Advanced

12.4%
Moderate

48.1%
Advanced

39.6%
Simple

12.4%
Moderate

APIs are a Favorite Vector for Bot Attacks

Over the past year, automated threats caused **30%** of API attacks. Among them, **17%** were bad bots exploiting business logic vulnerabilities, while **13%** were other types of automated threats. Business logic attacks exploit flaws within an application's design and implementation, allowing attackers to manipulate legitimate functionality and potentially gain access to sensitive data or user accounts.

The use of APIs for seamless communication between different applications and services is increasing, making them a critical element of software development. Due to their machine-readable nature, APIs are increasingly susceptible to bad bot attacks, with a lack of visibility into API traffic making them challenging to detect. However, the widespread use of APIs also made them an attractive target for bad bots. Malicious bots take advantage of APIs, which often act as direct pathways to sensitive data, making them vulnerable to business logic abuse and fraud. APIs increase the attack surface, providing more entry points for automated attacks. Since organizations continue to rely heavily on APIs, it's essential to implement robust security measures to protect against these sophisticated threats.

The Bad Bot Problem is a Cross-Industry, Cross-Functional One

Bad bots pose a grave threat to various industries and organizational functions. They can carry out malicious activities at a speed and scale beyond human capacity, making them a favored tool for abuse, misuse, and attacks.

While some bad bot use cases, such as content scraping and account takeover, are common across industries, others, like scalping, usually affect specific sectors like online retail and entertainment (ticketing). Some industries, like airlines, have unique use cases, such as 'seat spinning' attacks (see "Bad bot Traffic by Industry" section for more information).

Largest share of Bad Bot Traffic by Industry in 2023

Gaming	**57.2%**
Telecom & ISPs	**49.3%**
Computing & IT	**45.9%**
Travel	**44.5%**
Community & Society	**42.2%**

Largest share of Advanced Bad Bot Traffic by Industry in 2023

Law & Government	**75.8%**
Entertainment	**70.8%**
Financial Services	**67.1%**
Travel	**60.9%**
Gambling	**52.3%**

Residential Proxies are the Latest Tool in the Arsenal of Advanced Bot Operators

Bad bot traffic originating from residential proxies accounted for just over a quarter of all bad bot traffic. Residential proxies allow bot operators to evade detection by making it appear as if the origin of the traffic is a legitimate, ISP-assigned residential IP address. Doing so makes it more difficult for websites and online platforms to differentiate between genuine user interactions and malicious bot behavior.

The popularity of mobile browsers among bad bot operators continues to increase. In 2023, **44.8%** of bad bots attempted to evade detection by disguising themselves as a mobile browser. Mobile ISPs also remained popular, accounting for **18.3%** of attacks launched.

Bad Bots report as mobile user agents (Mobile Safari, Mobile Chrome, etc.)	**44.8%**
Bad Bots launched from residential ISPs	**25.8%**
Bad Bots launched from mobile ISPs	**18.3%**

Bad Bots Across the Globe

The US saw an increase in attacks this past year after several years of declining attacks, accounting for **47%** of all bot attacks globally, up from **41.8%** in 2022. New to the top five this year, the Netherlands has overtaken Australia at the second spot, with **9%** of bot attacks targeting it. Australia dropped to third place, targeted by **8.4%** of attacks, down from **16.4%** last year and more in line with previous years.

Top 5
Most Targeted Countries by Bad Bots

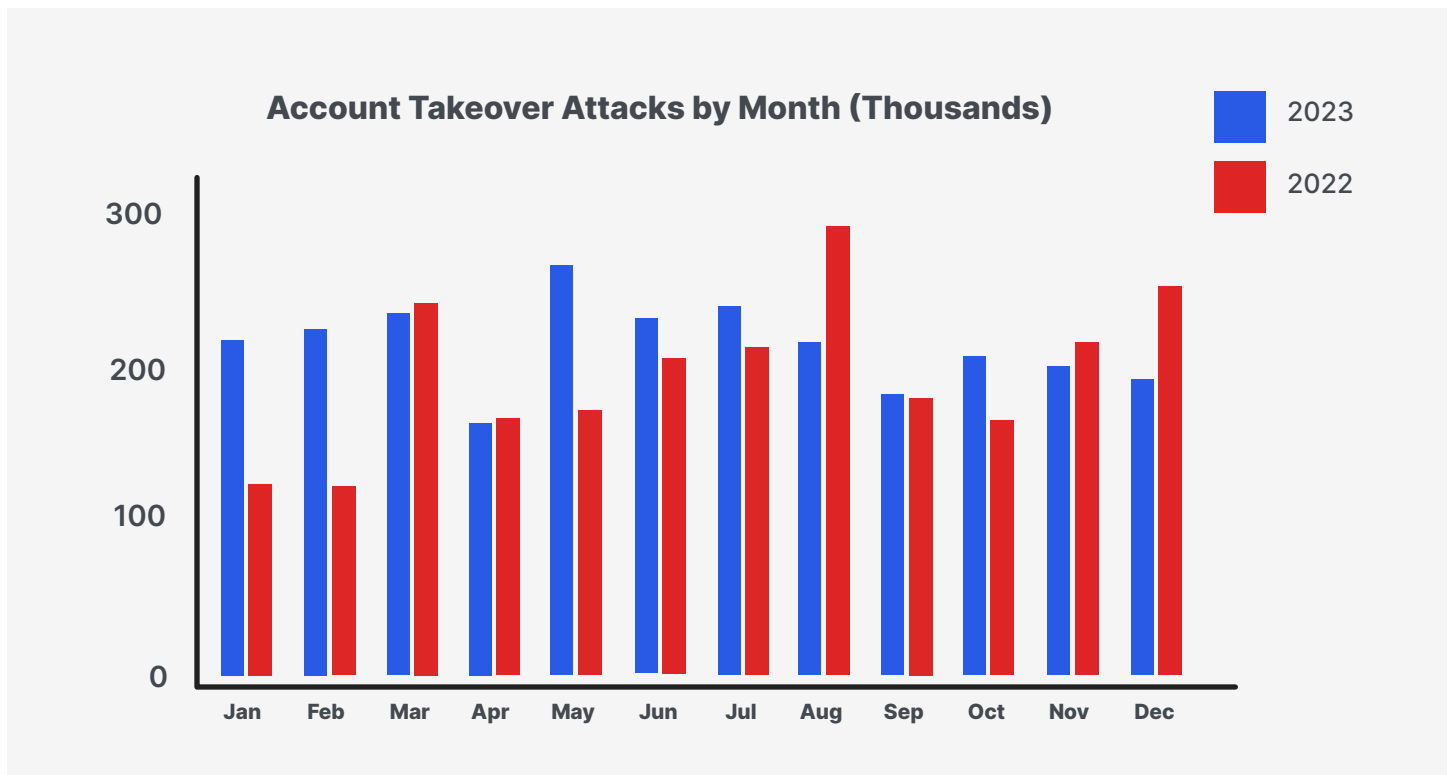| United States	47%
Netherlands	9%
Australia	8.4%
United Kingdom	5.1%
France	3.1%

Account Takeover Attacks

Account takeover (ATO) attacks are among the most prevalent automated threats. They involve using bots to attempt unauthorized access and takeover of user accounts through credential stuffing and credential cracking techniques, resulting in digital identity theft and significant losses for organizations. Losses from identity theft were estimated to reach $635.4 billion in 2023, according to Aite Group[2].

The following chart represents the monthly ATO attacks recorded by Imperva in the past two years. Attacks increased by **10%** between 2022 and 2023. While the number of attacks continues to grow, the growth is less significant than in previous years, despite a considerable increase of **77%** and **86%** in January and February, respectively. May and October also saw an increase in attacks compared to 2022 **(56% and 25%)**. The calendar year 2023 ended with fewer attacks.

August 2022 saw the highest number of attacks in the past two years. This increase is likely due to a **70%** increase in global data breaches around that time, as covered in last year's report.

Account Takeover Attacks by Month (Thousands)

Legend: ■ 2023 ■ 2022

---

2 https://aite-novarica.com/us-identity-theft-stark-reality#:~:text=Aite%20Group%20projects%20that%20losses%20from%20all%20identity,it%20from%20a%20simple%20fraudulent%20credit%20card%20transaction.

imperva.com

Almost Half of ATO Attacks Target APIs Directly

Account takeover attacks targeting APIs accounted for 44% of all ATO attacks recorded by Imperva, compared to **35%** last year. The widespread adoption of APIs due to the proliferation of mobile and web applications made them an appealing entry point for attackers seeking to compromise user accounts. These APIs handle crucial identity verification processes, making them an ideal target. However, implementing security measures is challenging due to the complexity of modern IT environments and the interconnected nature of online platforms. As a result, cybercriminals exploit vulnerabilities in authentication APIs to gain unauthorized access to user accounts. They use techniques such as credential stuffing, brute force attacks, or API abuse. The increasing frequency of account takeover attacks targeting authentication APIs highlights the need for organizations to enhance their API security measures and protect them against today's most sophisticated automated attacks.

Account Takeover Attacks by the Numbers

10% Growth in account takeover attacks between 2022 and 2023

11% Percentage of account takeover attempts out of all logins

44% Percentage of account takeover attacks that targeted APIs

Industries with the highest ATO ratio of all logins

Business Services	**38%**
Sports	**35%**
Food & Groceries	**33%**
Computing & IT	**24%**
Healthcare	**18%**
Travel	**17%**

Most targeted countries by ATO attacks

United States	**40%**
United Kingdom	**7%**
Germany	**7%**
Australia	**5%**
Spain	**5%**
Thailand	**4%**

Most-Attacked Industries

As opposed to the industries with the highest ratio of malicious logins out of all logins, the following chart illustrates what industries experienced the most significant volume of ATO attacks in 2023. Given the incentives behind user accounts, it is no surprise that, similar to last year, Financial Services was targeted the most, accounting for **36.8%** of attacks. The Travel industry was second **(11.5%)**, followed by Business Services **(8%)**, Computing & IT **(5.5%)**, Automotive **(4.7%)**, and Retail **(4.7%)**.

Account Takeover by Industry

36.8%
Financial Services

11.5%
Travel

8%
Business Services

7.5% Other
2.2% Lifestyle
2.4% Entertainment
2.5% Education
3.4% Law & Government
3.5% Gaming
3.6% Telecom & ISPs
3.7% Community & Social
4.7% Retail
4.7% Automotive
5.5% Computing & IT

imperva.com
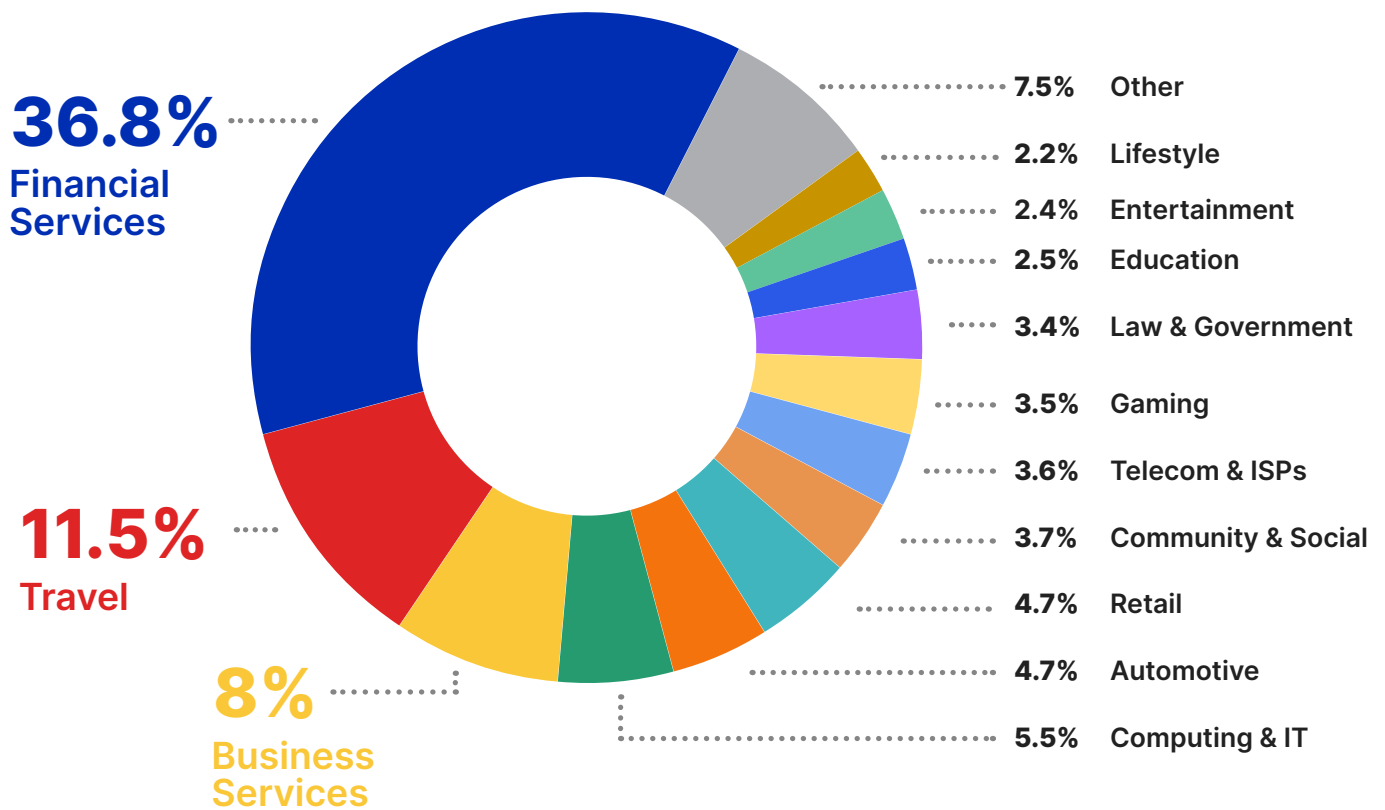
The Cost of Not Protecting Against Account Takeover

If you have a login page, the chances of it being targeted by an account takeover attack are high. The chances are even higher if valuable information or financial incentives are attached to your users' accounts. Still, many organizations stagnate on proactively preventing ATO attacks, the costs of which can be staggering. For example, consider a hypothetical scenario of an ATO attack on a website conducting business in the European Union (EU). The potential damages can skyrocket into the millions.

Under GDPR, regulatory fines can reach up to **4%** of a company's annual global turnover or €20 million, whichever is greater. For a company with an annual global turnover of $100 million, the maximum fine alone could be $4 million.

But the costs don't end there. If victims of a breach file a class action lawsuit, the total potential damages could reach $5 million, given an average claim of $500 per customer for 10,000 affected customers.

Reputational damage is another significant cost that's harder to quantify. A loss in customer trust can lead to reduced sales and a decline in stock value. If sales decline by **10%** over the next year for a company with an annual global turnover of $100 million, the loss could be another $10 million. A **5%** decline in stock value for a company with a market cap of $200 million equates to a $10 million loss.

Finally, additional costs, such as notification costs, legal and consulting fees, increased security measures, and credit monitoring services for affected customers, are to be considered. These could add up to another $2.5 million.

Under GDPR, regulatory **fines can reach up to 4% of a company's annual global turnover** or **€20 million,** whichever is greater.
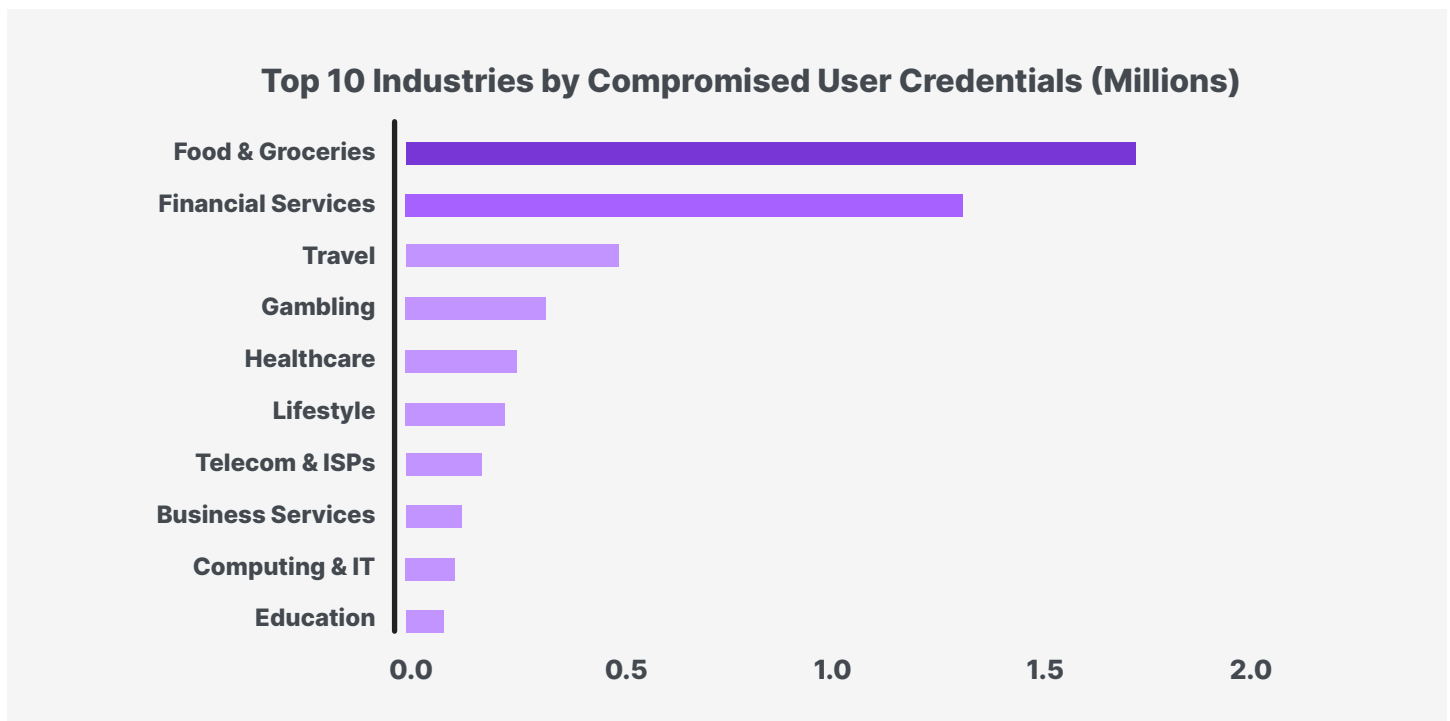
How Will Passkeys Affect the Prevalence of Account Takeover Attacks?

The introduction of Passkeys[3,4] aims to enhance the online user experience and reduce the risk of account takeover fraud. Passkeys are a more convenient and secure alternative to passwords. They work on all major platforms and browsers, enabling users to sign in by unlocking their computer or mobile device with their fingerprint, face recognition, or a local PIN. This alleviates the burden on users imposed by traditional passwords, mitigating the challenges of selecting and recalling strong passwords for multiple accounts.

By incorporating passkeys into the authentication processes, organizations can reduce the vulnerability of accounts to takeover attempts, strengthening their security posture and protecting user information. However, the widespread adoption of passkeys across various online platforms and services is necessary for their effectiveness. Organizations need concerted efforts to implement and integrate passkey systems into their authentication processes. As more organizations embrace the technology, it will be interesting to see its impact on the prevalence of account takeover attacks. There are early signs of a slowdown in growth regarding the number of attacks, although it is too soon to make definitive statements. One thing is clear: with the current state of security, account takeover remains a significant threat to organizations and end-users. Vigilance and proactive measures are crucial in safeguarding against potential attacks.

Compromised User Accounts

Detecting user accounts compromised in online data breaches can help organizations enhance security measures and prevent impending account takeover attacks. The chart below illustrates the top 10 industries with the most compromised accounts identified and alerted by Imperva.
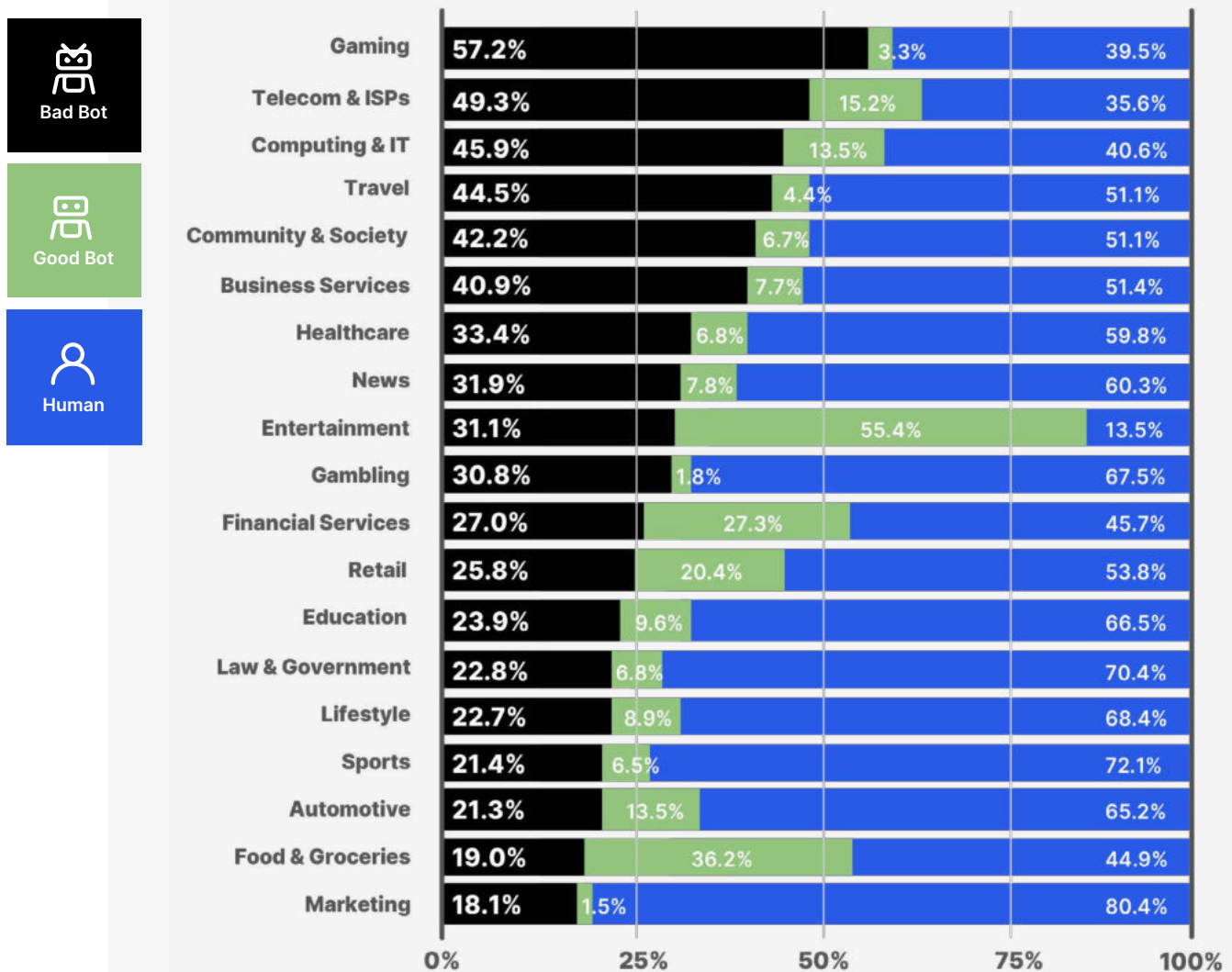

Top 10 Industries by Compromised User Credentials (Millions)

3 https://fidoalliance.org/passkeys/
4 https://developers.google.com/identity/passkeys

imperva.com

Bad Bot Traffic by Industry

Each sector has a different bad bot problem. The following chart represents the traffic profile that was recorded by Imperva during 2023 in a per-industry breakdown view, offering a closer look at how the overall increase in bad bot traffic levels affected each industry.

Bad Bot v Good Bot v Human Traffic 2023 - Industry Breakdown

Industry	Bad Bot	Good Bot	Human
Gaming	57.2%	3.3%	39.5%
Telecom & ISPs	49.3%	15.2%	35.6%
Computing & IT	45.9%	13.5%	40.6%
Travel	44.5%	4.4%	51.1%
Community & Society	42.2%	6.7%	51.1%
Business Services	40.9%	7.7%	51.4%
Healthcare	33.4%	6.8%	59.8%
News	31.9%	7.8%	60.3%
Entertainment	31.1%	55.4%	13.5%
Gambling	30.8%	1.8%	67.5%
Financial Services	27.0%	27.3%	45.7%
Retail	25.8%	20.4%	53.8%
Education	23.9%	9.6%	66.5%
Law & Government	22.8%	6.8%	70.4%
Lifestyle	22.7%	8.9%	68.4%
Sports	21.4%	6.5%	72.1%
Automotive	21.3%	13.5%	65.2%
Food & Groceries	19.0%	36.2%	44.9%
Marketing	18.1%	1.5%	80.4%

Legend: Bad Bot · Good Bot · Human

GAMING and video game websites sit at the top again in this year's Bad Bot Report. Similar to last year **(58.7%)**, a substantial percentage **(57.2%)** of traffic on gaming sites is generated by bad bots. Bots can cause trouble by taking over user accounts, creating fake accounts to exploit benefits, and cheating. They do difficult or impossible things for human players, such as performing high-speed interactions with a game to beat human players or farming virtual currency, items, or experience points (XP) continuously. These actions make it unenjoyable for genuine human players, who eventually leave, leading to a decline in active player numbers and engagement, which results in revenue loss.

The **COMPUTING & IT** industry saw an increase in bad bot traffic in 2023, accounting for **45.9%** of all traffic, which is higher than the previous year's level of **40%**. Bad bots harm the industry, leading to technical problems, fraud, and security risks. One of the most common ways bad bots target the sector is through Distributed Denial-of-Service (DDoS) attacks, whereby many bots inundate a website's servers with requests. Bad bots also scrape sensitive data, such as login credentials and personal information, which can lead to potential data breaches and identity theft. Additionally, bad actors use bots for vulnerability scanning and click fraud, leading to skewed metrics and revenue losses.

The **TELECOM & ISPs** sector experienced a slight increase in traffic from bad bots. In 2022, the percentage of bad bot traffic was **47.7%**, and rose to **49.3%** in 2023. This sector encompasses mobile ISPs, residential ISPs, hosting providers, and others. Bad bots target this industry with various malicious activities, including scraping sensitive customer data and brute force login attacks to take over user accounts. Since this industry is highly dependent on availability and sensitive to downtime, bad bots can launch Distributed Denial-of-Service (DDoS) campaigns to overwhelm their infrastructure and disrupt services. They often masquerade as legitimate users, making distinguishing between genuine and fake traffic hard. Furthermore, bot traffic can skew website analytics, leading to misguided decision-making.

The **TRAVEL** industry has fully recovered from several challenging years. More people are traveling than ever before[5,6]. Unfortunately, that also increases interest from bots, as travel websites have seen a significant uptick in bad bot traffic this year, going from **37.4%** of all web traffic to **44.5%**. The travel industry always struggled with complex bot problems because bad actors can exploit the various ways business logic is used in travel applications.

Within the travel sector, **airlines** are particularly targeted. The main problem stems from an airline's online platform, which includes its website, mobile app, and APIs. These platforms are where customers access flight information, make purchasing decisions, and book their flights. Unfortunately, bots often target these platforms to scrape data, disrupt services, and sometimes even commit fraud.

The leading issue airlines face is the large number of scraping bots that access their web properties without permission. These bots come from various sources, such as Online Travel Agencies (OTAs), aggregators, and competitors. The high volume of bots scraping flight information causes many problems, including damaging business insights like look-to-book ratios and increasing fees for third-party booking vendors. Last year, we shared the story of an airline that had its search API heavily scraped by bots for flight information. It resulted in over $500K in monthly charges for API requests by their third-party vendor. We're seeing similar attacks targeting other airlines this year.

A sudden change in the look-to-book ratio can indicate that bot traffic is actively scraping flight information. This is a significant issue for many airlines. While authorized OTAs and aggregators can scrape data under agreed terms, unauthorized ones use bots to scrape prices and flight information without an agreement. This unauthorized activity breaches the airline's terms and skews critical business metrics and insights.

Competing airlines also deploy bots to gather real-time market intelligence. Bots scrape competitor prices, seat inventories, and discounted fares, adding to the volume of bot traffic and serving no valuable purpose to the victim airline.

> **The most damaging bot activity comes from criminals who launch Bots to compromise loyalty rewards programs.**

The most damaging bot activity comes from criminals who launch bots to compromise loyalty rewards programs. These bots run brute-force credential stuffing and cracking attacks on login pages to gain access to accounts, steal loyalty points, and commit fraudulent purchases.

One bad bot use case unique to the airline industry is seat spinning. This issue is particularly prevalent in the Asia Pacific region. Seat-spinning bots hold seats without making a payment, often for up to 24 hours. These bots enable operators, such as unauthorized OTAs, to hold and resell bookings without investment. The impact is most visible as departure time approaches, with seemingly fully booked flights suddenly showing increasingly empty seats. Seat spinning leads to lost revenue and damages the airline's reputation.

Overall, the effects of bots on the airline industry are far-reaching. They lead to unauthorized scraping, seat spinning, account takeover, and fraud. These activities hamper customer experience and tarnish the airline's reputation. They can lead to poor website performance and even downtime if left unchecked.

5 https://www.washingtonpost.com/climate-environment/2023/11/23/pandemic-flying-normal-emissions/
6 https://www.euronews.com/travel/2023/04/21/post-covid-revenge-travel-has-gone-big-and-the-revenge-is-sweet

COMMUNITY & SOCIETY websites had **42.2%** of traffic from bad bots, a slight increase from **41.4%** last year. One of the most common types of bad bots is spam bots, also known as Fake News Spam and Comment Spam. These bots spread fake news, amplify propaganda, and conceal malicious content like malware within clickbait links. This issue is prevalent even among nonprofit organizations that accept donations on their websites. Bots exploit their donation pages to test stolen credit card numbers, which puts a lot of financial burden on nonprofits.

The **HEALTHCARE** sector has seen a rise in bad bot traffic, with **33.4%** of website traffic originating from bad bots, compared to **31.7%** in the previous year. Bad bots that target the healthcare sector usually aim to obtain sensitive customer data, which can result in data breaches. These bots can also take control of user accounts to access medical records or scrape confidential health information, such as patient records, medical history, and insurance details. This stolen data can be sold on the dark web for profit or used for fraudulent activities. Moreover, bad bots in healthcare pose a threat by overloading systems through Distributed Denial-of-Service (DDoS) attacks, which make it challenging for patients and healthcare providers to access critical information and services.

FINANCIAL SERVICES saw bad bots account for **27%** of site traffic in 2023. Interestingly, almost the same proportion of traffic came from good bots. This can result from financial aggregators and other service providers using bots to provide end users with valuable information and insights. But when it comes to bad bots, the sector faces a significant threat from account takeover attacks. Bad bots use brute-force login techniques such as credential stuffing or credential cracking to attempt illegal access to user accounts. Other common threats include credit card fraud and custom content theft, such as frequently changing interest rates. Another automated threat targeting the industry is arbitrage bots that target cryptocurrency exchanges and NFT marketplaces. These bots use web scraping to identify imbalances in pricing between different exchanges and marketplaces. They help operators trade crypto and NFTs from one exchange or marketplace to another, taking advantage of pricing differences between the same coin or pairs on different exchanges to make a profit.

The **RETAIL** industry had just over a quarter **(25.8%)** of website traffic from bad bots. This is an increase from **22.7%** in the previous year. Like last year, online retailers also experienced a high volume of good bot traffic **(20.4%)**. This is most likely due to the prevalence of price comparison crawlers used by search engines and websites. Online retailers face various forms of automated threats that negatively impact their business and disrupt customer experience and operations. Bad bots are used for a variety of malicious activities, such as scraping data by competitors, obtaining limited availability items for resale at higher prices (scalping), carrying out Distributed Denial-of-Service (DDoS) attacks, and engaging in criminal activities such as credit card cracking, carding, gift card cracking, and account takeover (ATO). Account takeover (ATO) attacks have increased during this year's holiday season. ATO attacks have increased since September, with a significant spike in attack activity recorded on November 8, 14, and 24 (Black Friday). The number of attacks on Black Friday saw an astonishing **85%** increase, compared to a **66%** increase in ATO attacks during Black Friday 2022. Furthermore, the intensity of these attacks is also increasing, with the number of malicious login requests soaring by **82%** between October and November.
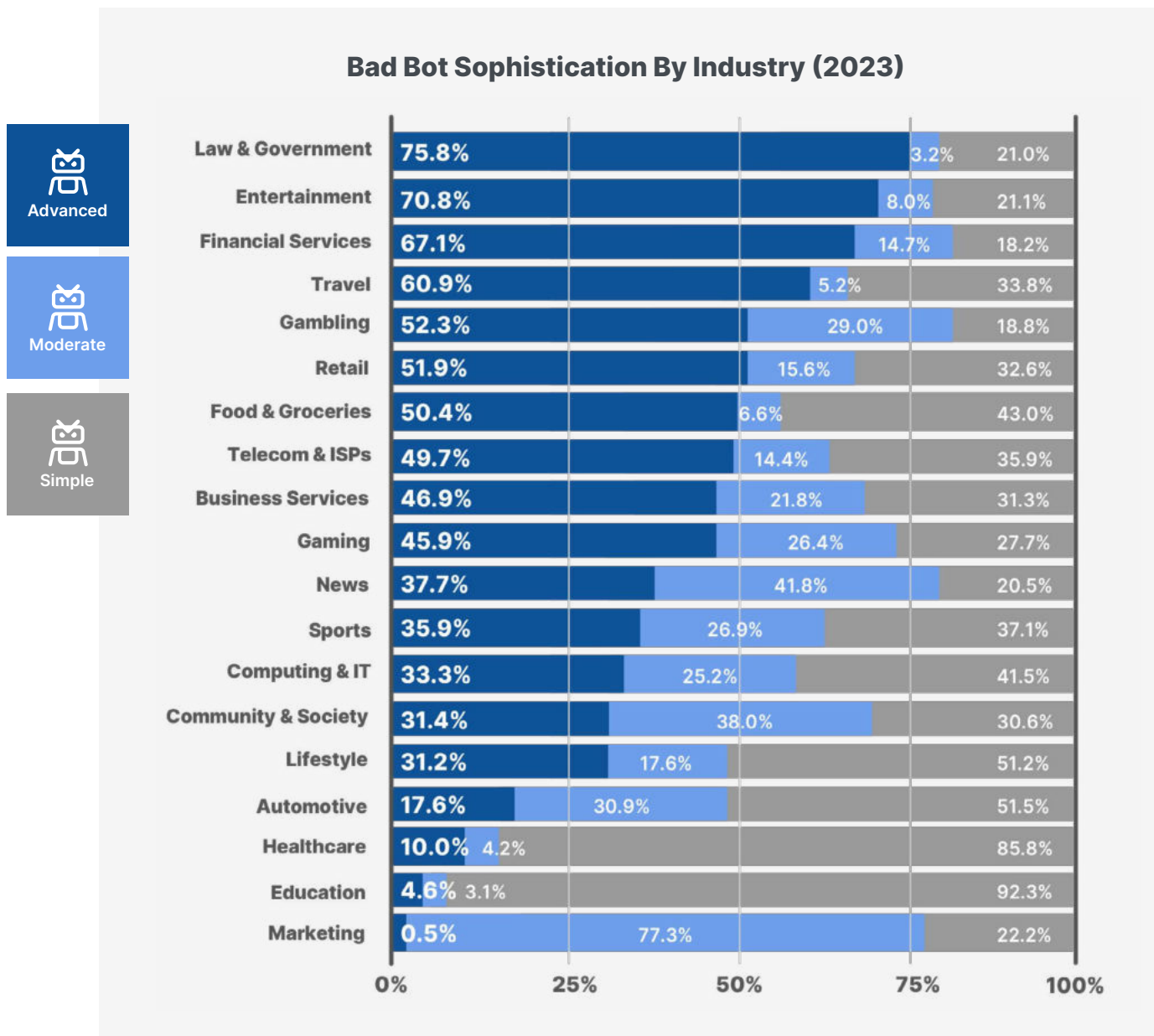
The **ENTERTAINMENT** sector includes ticketing platforms, streaming services, production companies, and event venues. Like last year, the industry saw a very high volume of automation, both good **(55.4%)** and bad **(31.1%)**, amounting to **86.5%** of all traffic, up from **83.4%**. The reason for the high volume of good bots can be related to the various third parties scraping entertainment websites to provide price comparisons, availability information, and recommendations to consumers. The most targeted websites across this sector are ticketing sites. Entertainment was among the first industries targeted by bad bots. Scalping bots, seat inventory checkers, and credential-stuffing bots that access user accounts are the most prevalent bots on these sites.

Bad Bot Sophistication by Industry

The following chart shows a breakdown of bad bot traffic based on their sophistication levels. The higher the proportion of advanced bad bots, the more complex the bot problem becomes for the industry. This comprehensive analysis sheds more light on the bad bot risks different sectors faced this year.

It is crucial to understand that there isn't necessarily a correlation between the sophistication of bad bot traffic and the traffic volume itself. In other words, an industry with a large amount of bad bot traffic may have all of it classified as simple bots. However, it is essential to remember that advanced bot traffic poses a significant risk, no matter how small in volume. This is because advanced bad bots can achieve their goals with fewer requests than simpler bad bots and are much more persistent in staying on their designated target.

Bad Bot Sophistication By Industry (2023)

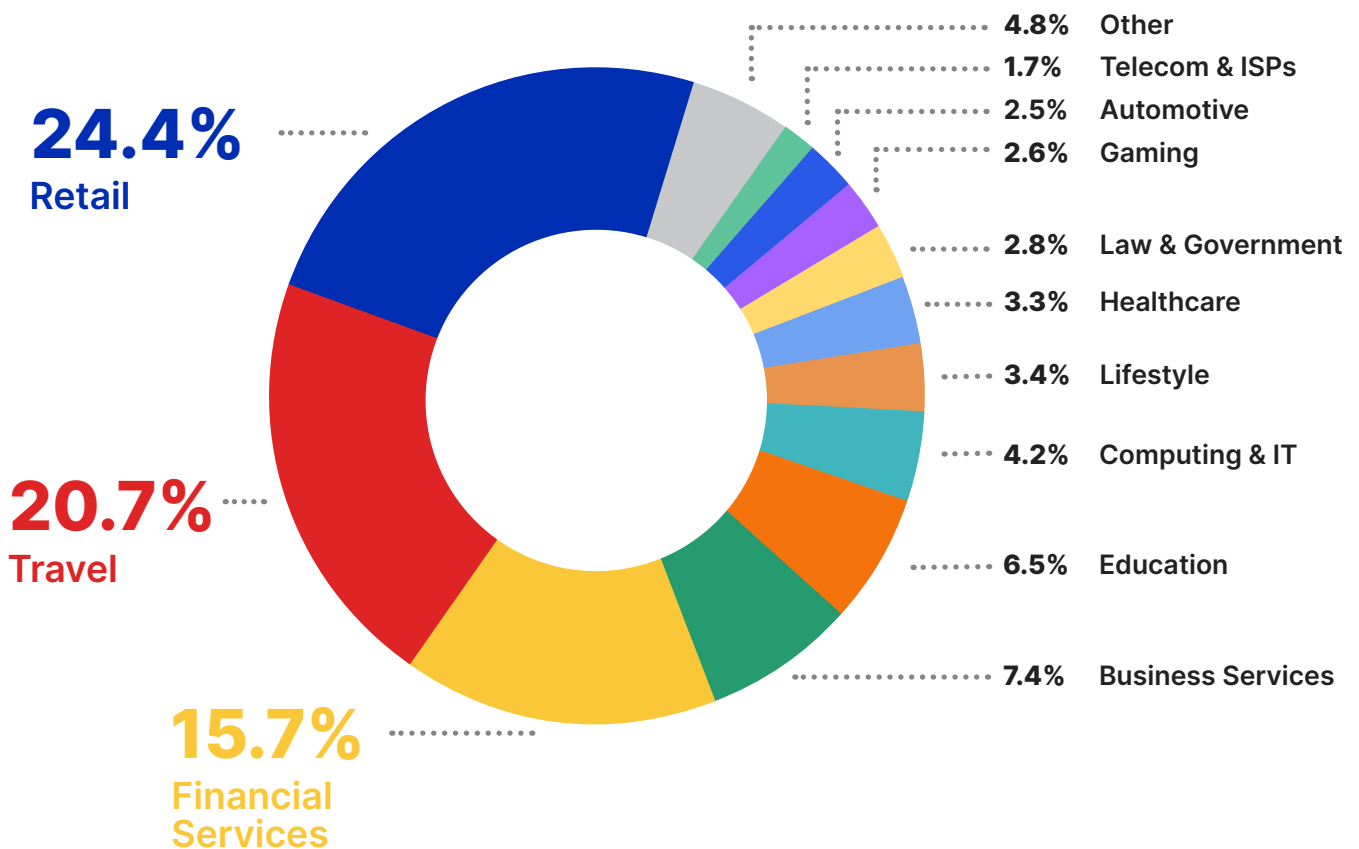| Industry	Advanced	Moderate	Simple
Law & Government	75.8%	3.2%	21.0%
Entertainment	70.8%	8.0%	21.1%
Financial Services	67.1%	14.7%	18.2%
Travel	60.9%	5.2%	33.8%
Gambling	52.3%	29.0%	18.8%
Retail	51.9%	15.6%	32.6%
Food & Groceries	50.4%	6.6%	43.0%
Telecom & ISPs	49.7%	14.4%	35.9%
Business Services	46.9%	21.8%	31.3%
Gaming	45.9%	26.4%	27.7%
News	37.7%	41.8%	20.5%
Sports	35.9%	26.9%	37.1%
Computing & IT	33.3%	25.2%	41.5%
Community & Society	31.4%	38.0%	30.6%
Lifestyle	31.2%	17.6%	51.2%
Automotive	17.6%	30.9%	51.5%
Healthcare	10.0%	4.2%	85.8%
Education	4.6%	3.1%	92.3%
Marketing	0.5%	77.3%	22.2%

imperva.com

Most Targeted Industries by Bot Attacks

The traffic profile breakdown for each industry shows the ratio of bot traffic to all traffic. In contrast, the distribution of bot attacks across industries gives a different perspective. It indicates which industries were targeted by the largest share of bot attacks. Like last year, Retail, Travel, and Financial Services are the top three most targeted industries.

As the previous section details, these industries face a complex bot problem, with various bot use cases threatening their bottom lines. All three rank high in the sophistication of bots on their sites.

It is important to note that an industry with a high ratio of bad bots does not necessarily correspond to being targeted more or less than other industries. An industry may have a low ratio of bot traffic because it experienced significant human traffic throughout the year. Or, it may have been targeted by more advanced bad bots that require fewer requests to achieve their desired outcomes.

Most Targeted Industries by the Number of Attack Requests

4.8%	Other
1.7%	Telecom & ISPs
2.5%	Automotive
2.6%	Gaming
2.8%	Law & Government
3.3%	Healthcare
3.4%	Lifestyle
4.2%	Computing & IT
6.5%	Education
7.4%	Business Services

24.4% Retail

20.7% Travel

15.7% Financial Services

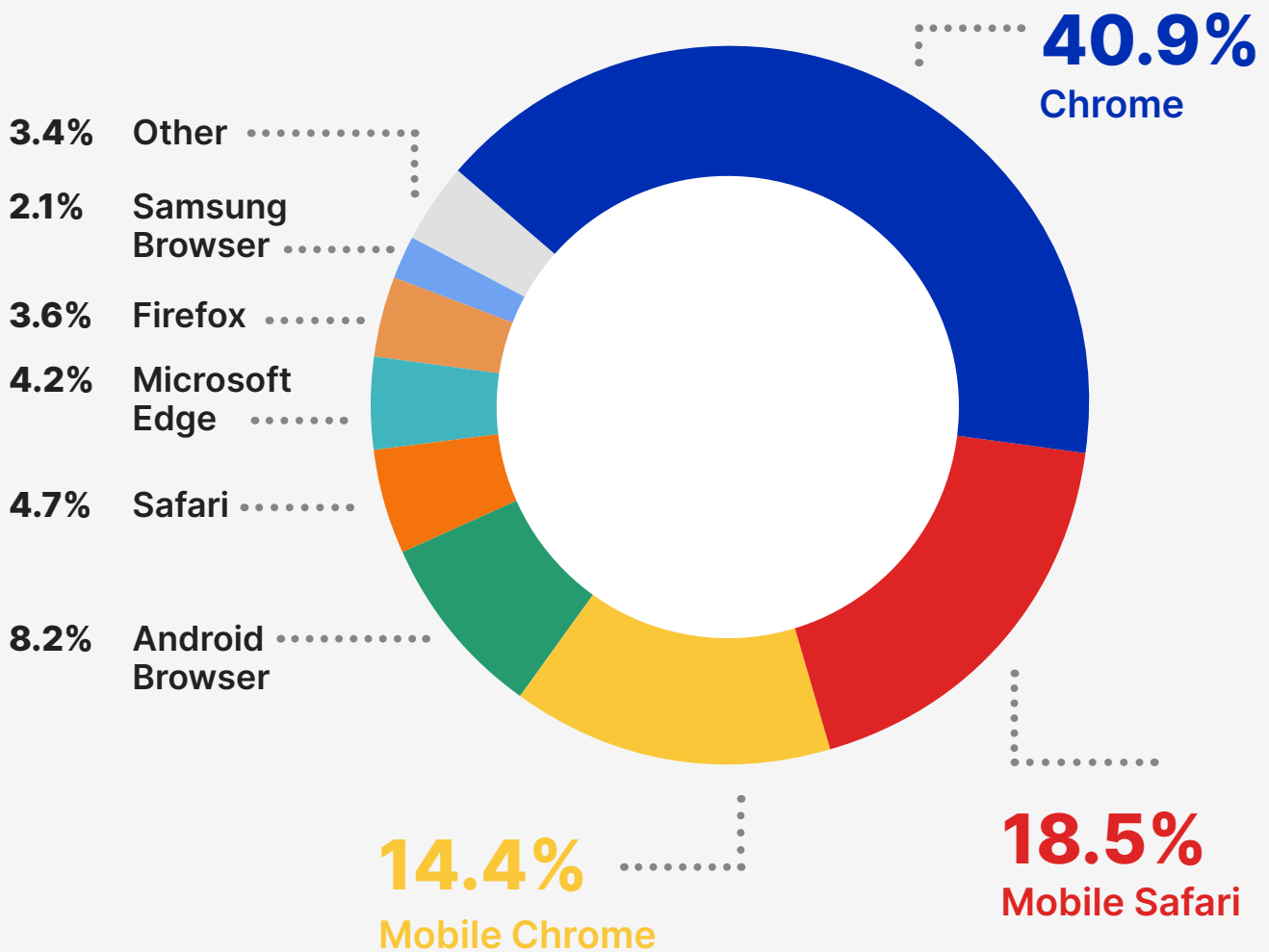# Mobile Chrome and Android Browser Increased in Popularity

Bad bots use various techniques to evade detection, one of which is to disguise themselves as legitimate users by reporting themselves to the origin as a web or mobile browser commonly used by humans. They achieve this by using browser automation software. This technique has become common among most bad bots, although it was once an advanced evasion method. Interestingly, the trend in browser popularity among bad bots has changed over the past decade, reflecting changes in human user preferences and other trends that help bots evade detection. For example, Internet Explorer was once a popular browser among humans and bad bots, but this is no longer true.

Top Self Reporting Browsers by Bad Bots 2013-2023

Legend:
- Chrome
- Firefox
- Mobile Safari
- Mobile Chrome
- Safari
- Android Browser
- Internet Explorer
- Microsoft Edge

Browser	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Chrome	22.90%	26.60%	26.90%	38.60%	45.50%	49.90%	55.40%	33.30%	42.70%	40.40%	40.87%
Firefox	27.20%	26.60%	17.70%	22.90%	26.90%	17.50%	13.30%	26.50%	13.40%	5.00%	4.23%
Mobile Safari			5.00%	9.00%	5.70%		4.80%	11.80%	16.10%	20.20%	18.51%
Mobile Chrome	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	10.30%	11.90%	13.20%	14.38%
Safari	6.70%			7.60%	4.20%	6.60%	7.10%	4.60%	3.90%	5.50%	4.60%
Android Browser		4.90%	4.40%		8.80%		7.90%	3.50%	4.40%	4.10%	8.25%
Internet Explorer	22.90%	23.30%	11.90%	6.70%	6.50%	4.10%	3.70%	3.50%	.90%	.30%	.21%
Microsoft Edge	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	5.00%	2.23%

Over the past two years, we have witnessed an increase in the popularity of mobile web browsers amongst bad bots. It started with the increase in popularity of bad bots opting for Mobile Safari **(18.51%)** as their browser of choice but rapidly expanded to Mobile Chrome **(14.38%)** and Android Browsers **(8.25%)**.

Chrome usage by bad bots remains the same at **40.87%** of all bad bot traffic, while Firefox continues to lose popularity **(3.57%)**.

Most Targeted Industries by the Number of Attack Requests

3.4% Other
2.1% Samsung Browser
3.6% Firefox
4.2% Microsoft Edge
4.7% Safari
8.2% Android Browser

40.9% Chrome
18.5% Mobile Safari
14.4% Mobile Chrome

Mobile User Agents
Account for Almost Half of Bot Traffic

Bad bots masquerading as mobile user agents accounted for **44.8%** of all bad bot traffic. Their popularity increased drastically, from **28.1%** in 2020 to **44.8%** in 2023. There are two main reasons for this increase in popularity: first, bad bots attempt to closely mimic human traffic attributes. As of February 2024, over **55%** of internet traffic comes from mobile devices[7]. More of us use our mobile phones to browse the internet, so it would only make sense for bots to do the same to blend in with the human traffic. The split between mobile and desktop-based agents is very close when looking at bad bot traffic.

The second reason is related to privacy. Some web browsers, such as Mobile Safari, have additional privacy controls and features that make it easier for bad bots to hide their true identities. This is because these browsers may send fewer attributes to the website's origin, which makes it more challenging to create an accurate fingerprint of the device.

The percentage of bad bots that self-report as desktop-based user agents like Chrome, Firefox, Safari, or Edge has decreased from **68%** in 2020 to **54%** in 2023.

The remainder of bad bot traffic, **1.2%**, has reported themselves as other user agents (e.g., Playstation, Nintendo, Smart TVs, etc.).

Bad Bot User Agent Types in 2023

54% Desktop

1.2% Other

44.8% Mobile

Bad Bot Reported User Agent Types in 2016-2023

Desktop:
- 2016: 75.90%
- 2017: 83.20%
- 2018: 78.10%
- 2019: 79.40%
- 2020: 68.00%
- 2021: 60.90%
- 2022: 55.60%
- 2023: 54.00%

Mobile:
- 2016: 16.10%
- 2017: 10.40%
- 2018: 13.90%
- 2019: 12.90%
- 2020: 28.10%
- 2021: 35.60%
- 2022: 39.10%
- 2023: 44.80%

Other:
- 2016: 8.00%
- 2017: 6.40%
- 2018: 8.00%
- 2019: 7.70%
- 2020: 3.90%
- 2021: 3.50%
- 2022: 5.30%
- 2023: 1.20%

Legend:
- Desktop
- Mobile
- Other

7 https://explodingtopics.com/blog/mobile-internet-traffic

imperva.com

The Rise of Residential Proxies

This year, bad bot traffic originating from residential ISPs accounted for **25.8%** of all bad bot traffic, up from **17.4%** last year. While in the past, masquerading as a legitimate human user by appearing as a user agent (browser) commonly used by legitimate users was considered an advanced evasion technique, it is now a commodity. Hiding the origin of the request using a mobile or residential proxy kicks things up by adding another dimension of authenticity. This type of bot behavior differentiates sophisticated, persistent, and determined adversaries with the means and capabilities to achieve their goals from the less sophisticated ones.

The Imperva Threat Research Team has found that bot programmers increasingly use residential IP proxy integrations within their managed software offerings (e.g., All-in-One bots) and collaborative knowledge bases. We have been developing targeted detection mechanisms to detect and counter this evasion technique.

Although data centers remain the source of most bot attack traffic **(55.9%)**, traffic originating from them has decreased this year after a surprise increase last year. In 2020, data centers accounted for **54%** of bad bot traffic, dropping to **45.1%** in 2021. Then it significantly increased to **58.6%** of all bad bot traffic in 2022. This year, however, their number decreased.

The traffic originating from mobile ISPs decreased from **24.1%** in 2022 to **18.3%** in 2023.

Bad Bot Traffic by ISP Type 2023

55.9%
DC

18.3%
Mobile

25.8%
Residential
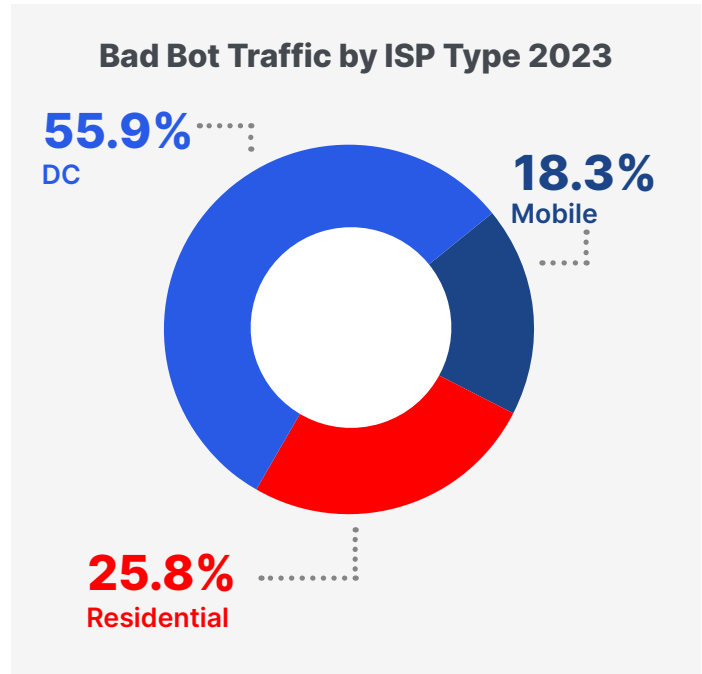
Bad Bot Traffic Originating from Mobile and Residential ISPs Claim Top Spots

As we just covered, mobile and residential proxies have become increasingly popular among bad bot operators. China Telecom has claimed the second spot, Comcast is number 4, and Spectrum is number 6. However, Amazon still holds the number one position, with 17.01% of bot traffic.
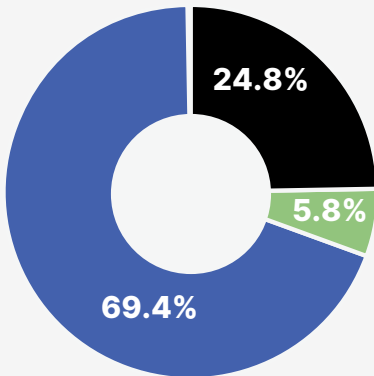
Top Bot Originating ISPs

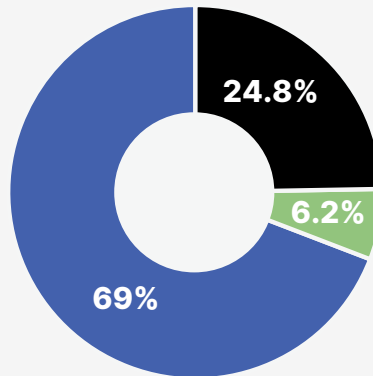| ISP	% of Bot Traffic
Amazon.com	**17.01%**
China Telecom	**3.42%**
Digital Ocean	**2.78%**
Comcast Cable	**1.76%**
Microsoft Azure	**1.63%**
Spectrum	**1.60%**
Safaricom	**1.51%**
Google Cloud	**1.51%**
Jio	**1.34%**
Contabo GmbH	**0.99%**

Bad Bots Across the Globe

Let's examine the traffic distribution at the national level. We have surveyed 13 countries and found that 6 out of 13 have experienced higher-than-average levels of bad bot traffic, exceeding the global average of **32%**. This year, Germany and Ireland again recorded over **60%** of traffic from bad bots. Similarly, the United States witnessed a slightly higher bad bot traffic ratio than the global, with **35.4%** of all traffic originating from bad bots.
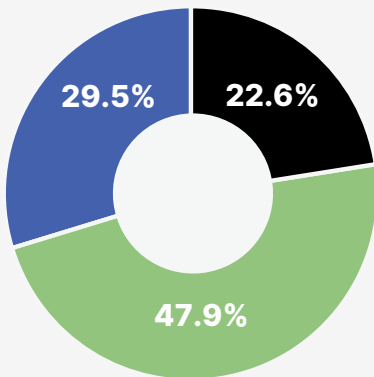
Bad Bot v Good Bot v Human Traffic 2023 - By Target Country

Ireland
- 71.4%
- 26.6%
- 2%

Germany
- 67.5%
- 25.5%
- 7%

Mexico
- 42.8%
- 46.9%
- 10.3%

China
- 39.7%
- 56.2%
- 4.1%

United States
- 38.4%
- 35.4%
- 26.2%

Singapore
- 35.2%
- 59.2%
- 5.6%

Australia
- 30.2%
- 63.7%
- 6.1%

Legend:
- Bad Bot
- Good Bot
- Human
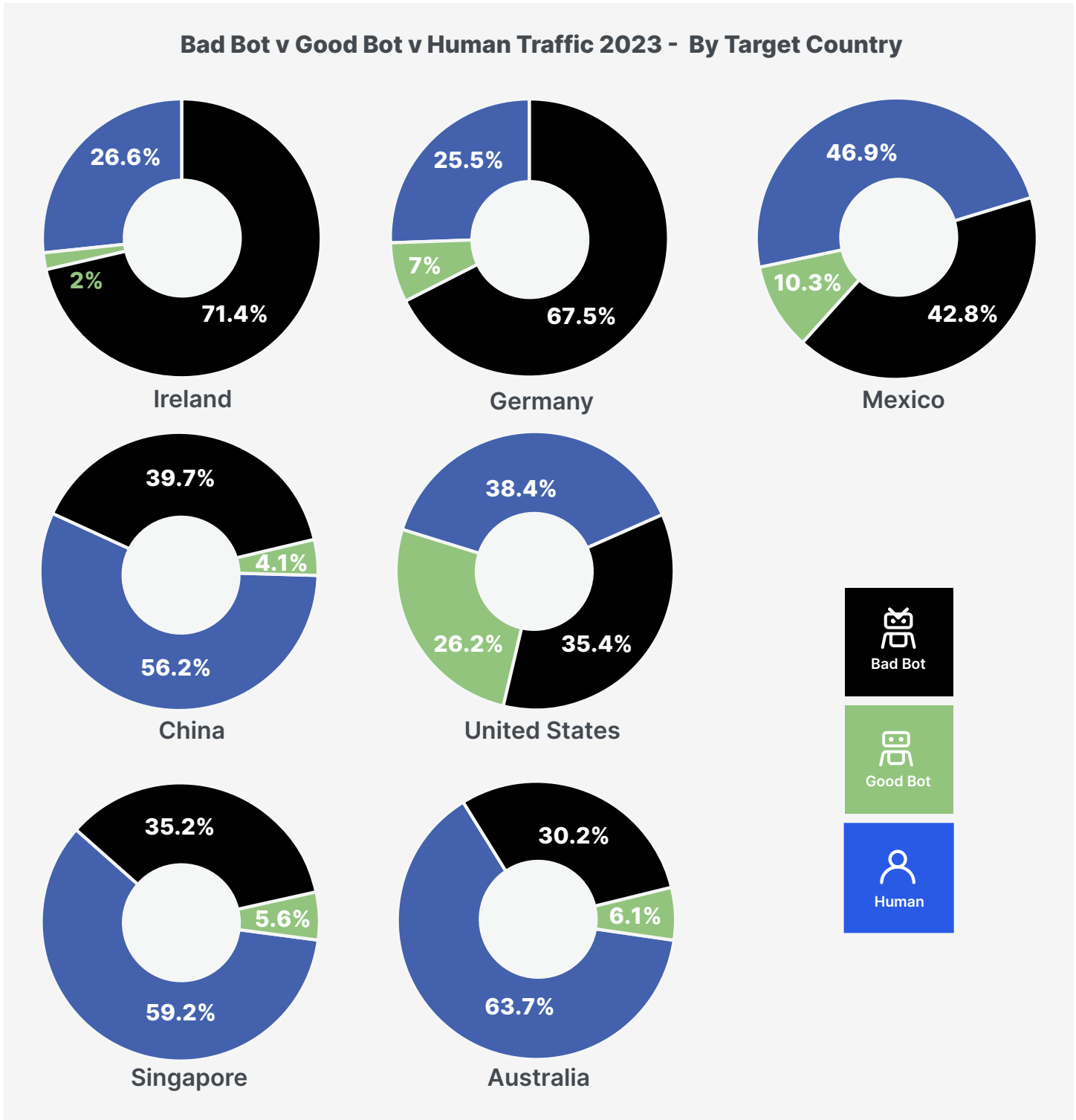
Bad Bot v Good Bot v Human Traffic 2023 - By Target Country

Canada
- 24.8% (Bad Bot)
- 5.8% (Good Bot)
- 69.4% (Human)

United Kingdom
- 24.8% (Bad Bot)
- 6.2% (Good Bot)
- 69% (Human)

Brazil
- 22.6% (Bad Bot)
- 47.9% (Good Bot)
- 29.5% (Human)

New Zealand
- 19% (Bad Bot)
- 19% (Good Bot)
- 62% (Human)

France
- 18.8% (Bad Bot)
- 6.1% (Good Bot)
- 75.1% (Human)

Japan
- 17.7% (Bad Bot)
- 16% (Good Bot)
- 66.3% (Human)
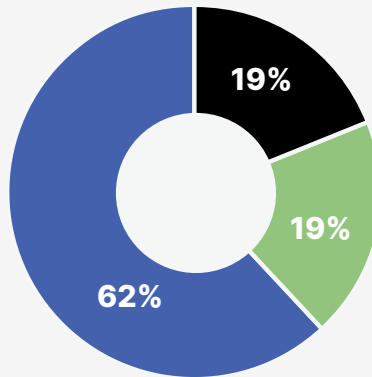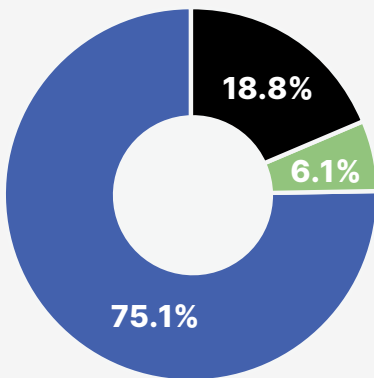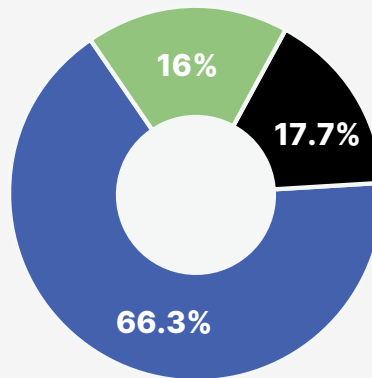
Legend:
- Bad Bot
- Good Bot
- Human
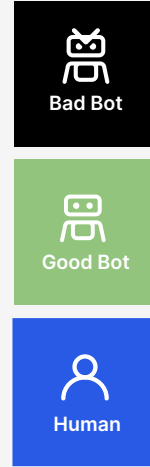
The United States and the Netherlands Were Targeted the Most by Bot Attacks

Bot attacks continue to target the United States, which remains the top priority target, with **47%** of attacks directed towards US-based websites. This percentage is an increase compared to last year, where **41.1%** of bot attacks were focused on the US. The Netherlands has surpassed Australia by a small margin this year, claiming the second spot with **9%** of bot attacks targeting it. Australia was targeted by **8.4%** of bot attacks, almost half of where it was last year **(16.4%)** but more in-line with the past **(6.8% in 2021)**. The United Kingdom was the fourth most targeted country with **5.1%** of attacks, followed by France, which was targeted by **3.1%**.

Top 10 Most Attacked Countries By Bad Bots

1 United States
2 Netherlands
3 Australia
4 United Kingdom
5 France
6 Singapore
7 Indonesia
8 Brazil
9 Canada
10 India

Bot Attacks Distribution by Target Country (2023)

- 13 % Other
- 1.6 % Columbia
- 1.6 % Hong Kong
- 1.7 % India
- 2.1 % Canada
- 2.2 % Brazil
- 2.2 % Indonesia
- 3.0 % Singapore
- 3.1 % France
- 5.1 % United Kingdom

47% United States

8.4% Australia

9% Netherlands
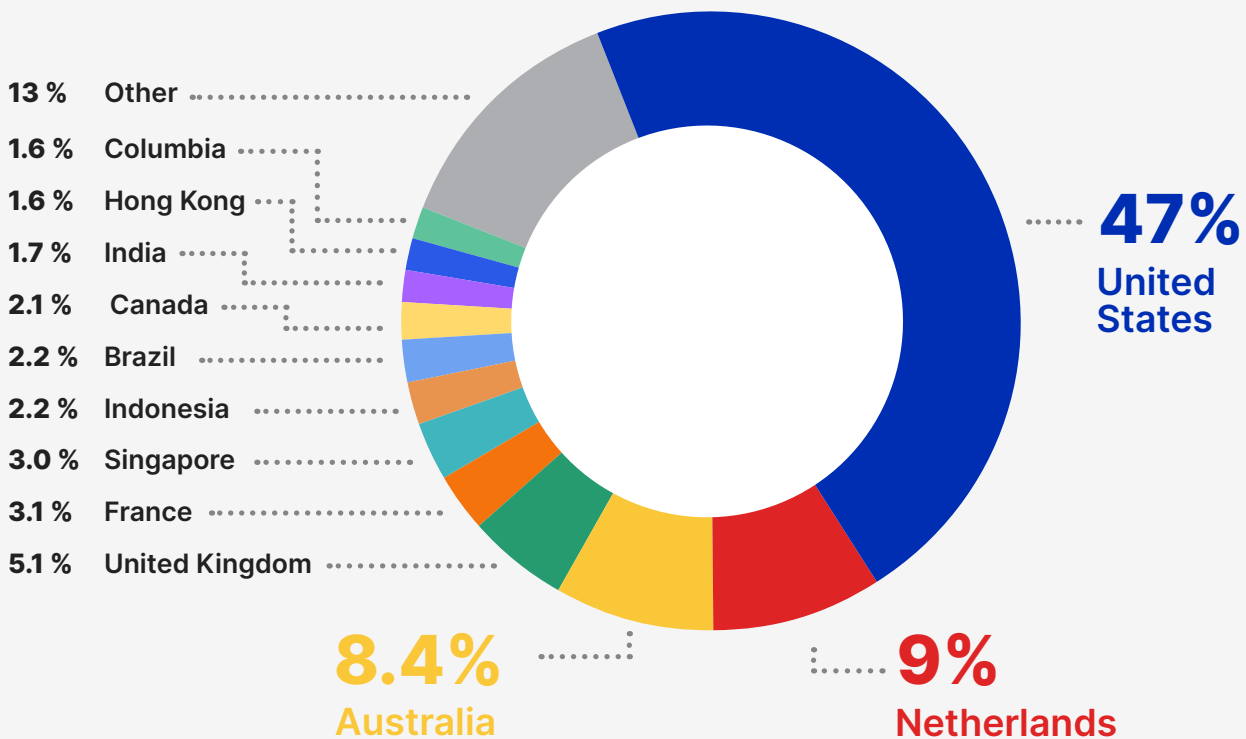
Bad Bots in the Age of Artificial intelligence

The rise of artificial intelligence (AI) and Large Learning Models (LLMs) is changing our lives in more ways than we can count. From enhancing business operations to making our daily lives more convenient, these technologies are changing the game. However, the rise of AI and LLMs also brings many challenges.

We've already covered the high-level implications of the issue on the profile of internet traffic throughout the report. These implications include the rising levels of automated traffic and the clear distinction between simple and advanced bad bots, all covered in the executive summary. Yet some challenges are more complex, like the renewed debate on the legality of web scraping, a contentious issue that was simmering for years.

Web scraping, the practice of using bots to extract data from websites, isn't new. However, the advent of AI and LLMs has brought this issue back into the spotlight. These advanced technologies rely heavily on vast data for training, often obtained through web scraping. While this practice can fuel AI development, it raises significant legal and ethical concerns.

The legality of web scraping largely depends on the jurisdiction and specific circumstances. However, the advent of AI has complicated the matter further. While some argue that the data is necessary for advancing AI technologies, others contend it infringes on copyright laws and privacy rights.

AI and LLMs has brought **web scraping back into the spotlight.**

The core of the debate lies in the use of proprietary content and data in training AI models. Many organizations argue that their intellectual property rights are being infringed upon when their data is scraped without permission. On the other hand, proponents of web scraping contend that the practice is essential for advancing AI and machine learning technologies.

This tug-of-war between innovation and privacy has led to a renewed debate on the legality of web scraping. The laws governing this practice are often outdated and vary significantly from country to country, making it a complex issue. As AI and LLMs continue to evolve, there's an urgent need for updated laws and regulations that balance fostering technological advancement and protecting proprietary content and data.

In a groundbreaking legal case, The New York Times has filed a lawsuit against OpenAI and Microsoft, alleging copyright infringement through web scraping to train AI models. OpenAI argues that its actions are protected under the "fair use" doctrine of the US Copyright Act. At the same time, The Times contends that OpenAI's use of its content does not meet the "transformative" criteria required for fair use. The outcome of this lawsuit could redefine the boundaries of copyright laws and AI, potentially setting a precedent for the legality of using copyrighted material for AI training. It also underlines the urgent need for updated copyright laws that balance content creators' rights with AI innovation's demands. This case highlights the complex legal and ethical challenges posed by web scraping in the age of AI, emphasizing the need for businesses to protect their digital assets proactively.

As AI continues to evolve, the need for clear legal guidelines balancing the needs for data with respect for copyright laws and privacy rights has never been more critical. The debate is far from over, and as we move forward, businesses, legal systems, and technology leaders must navigate this complex landscape with caution and responsibility.

Restaurant Reservations are the New Hotness

There is a simple rule of thumb or an equation regarding scalping bots: high demand plus limited availability equals bot interest. These bot operators are highly opportunistic and will take advantage of any situation where supply is scarce and demand is high. We've even seen bots snagging passports, visas, and driver's test appointments across the globe due to the backlog created by the pandemic between 2020 and 2022.

So, it is no surprise that they now target the restaurant industry by snapping up prime-time reservations and selling them at exorbitant prices on third-party platforms. In a digital era where convenience reigns supreme, online reservations have become the norm for securing a spot at your favorite eateries.

Imagine planning a special dinner at a top-tier restaurant, only to discover that all the slots are gone within milliseconds of release. Worse still, these reservations later appear on resale platforms,

High Demand Plus Limited Availability

=

Bot Interest

forcing you to pay up to $340 to secure an initially free spot. This is the reality for many diners today, thanks to the nefarious activities of bad bots.

Just as they've done with concert tickets and collectible sneakers, these bots exploit the system for profit, making it nearly impossible for genuine customers to secure reservations at popular establishments. This not only frustrates customers but also hurts the restaurant business. When bot-booked seats go unfilled, eateries lose out on potential revenue from empty tables and cancellation fees charged to invalid credit cards.

In response, restaurants and reservation platforms are waging a war against these cyber threats. They're implementing measures to detect and block suspicious activities, such as bookings from accounts with jumbled email addresses or disconnected phone numbers. Some are even reducing the number of online reservations, choosing to welcome more walk-ins instead.

Ticket Scalping Surges in a Post-Pandemic Era

Live events have made a triumphant return in the past couple of years, with extraordinarily high demand for concert tickets globally. As mentioned earlier, high demand plus limited availability equals bot interest. Indeed, there was a significant resurgence of ticket scalping (purchasing event tickets in bulk to resell at inflated prices). This age-old practice, nowadays powered by automation (aka bots), has found new life in the post-pandemic era.

The evolution of technology has transformed scalping techniques, with advanced bots now being the preferred tool for scalpers. Entertainment websites, where ticketing platforms are categorized, have seen the second-highest ratio of advanced bad bots this past year at **70.8%** (see 'Bad bot sophistication by industry' section).

These bots are usually all-in-one (AIO) 'solutions,' enabling their operators to automate the purchase process entirely. They often incorporate multiple evasion techniques and CAPTCHA-solving capabilities. This is causing widespread frustration among consumers and posing significant challenges for businesses and the live entertainment industry.

Businesses face potential revenue loss as genuine customers cannot purchase tickets at their original price, damaging their reputation and customer loyalty. Conversely, consumers have to contend with exorbitant prices and limited access to events, leading to frustration and potential mistrust in the market.

The surge in demand for live entertainment as pandemic restrictions eased has only fueled the resurgence of ticket scalping. This has led to several countries implementing legal measures to combat this issue. However, just as with the legality of web scraping, it's clear that businesses can't wait for legal measures to be put in place, as they must take proactive measures to mitigate the risks posed by bot traffic.

The evolution of technology has transformed scalping techniques, with **Advanced Bots now being the preferred tool for scalpers.**

How should businesses protect themselves from bots and online fraud? A universal solution can be elusive, given each site's unique vulnerabilities and attack vectors. Nonetheless, adopting a proactive approach by implementing multifaceted security measures can significantly mitigate the risk. This includes deploying advanced bot detection and cyber security management solutions. Together, these strategies form a comprehensive defense mechanism against the ever-evolving landscape of online fraud and bot-related security threats.

Security Recommendations for the Detection of Bad Bot Activity and Automated Fraud

1. Risk Identification

Stopping bot traffic begins with identifying potential risks to your website:

A. Marketing and eCommerce initiatives often attract an increased presence of bots, particularly during the launch of limited-quantity, high-demand products. Whether the latest sneakers, next-gen gaming consoles, or exclusive collector's items, specifying a launch date for these coveted products is a beacon for bots. These automated entities aim to secure the merchandise before genuine customers can, potentially monopolizing access and undermining your sales efforts. It's crucial to fortify your website's defenses to effectively manage the surge in traffic, ensuring you can distinguish between legitimate consumers and evasive bots intent on hijacking the product launch. Implementing advanced traffic analysis, real-time bot detection mechanisms and robust authentication measures can help safeguard your platform, ensuring fair access for actual customers.

B. Recognizing potential vulnerabilities on your site is a crucial element of an effective bot management strategy. Certain website features are particularly susceptible to malicious bot activities. For instance, incorporating login capabilities can lead to Credential Stuffing and Credential Cracking attacks, where attackers use stolen credentials to gain unauthorized access. Similarly, the presence of a checkout form

can escalate the risk of credit card fraud, known as Carding or Card Cracking. Furthermore, implementing gift card functionalities can attract bots intent on committing fraud. To mitigate such risks, it is essential to apply enhanced security measures and enforce stricter rules on these pages. Implementing multi-factor authentication, CAPTCHAs, and continuous monitoring for suspicious activities can significantly strengthen your site's defenses against these automated threats.

2. Vulnerability Reduction

Securing exposed APIs and mobile applications is as crucial as safeguarding your website, emphasizing the need for a holistic cybersecurity strategy encompassing all digital touchpoints. It takes more than just focusing on your website's security. APIs and mobile apps often serve as gateways to your web applications and sensitive data, presenting additional vectors for cyber threats. Implementing robust security measures across these platforms and blocking between systems is essential to reducing vulnerabilities. This integrated approach ensures a unified defense mechanism against potential attacks, minimizing the risk of unauthorized access to your web applications and critical data through any digital entry point.

3. Threat Reduction: User-Agents

Many bot tools and scripts contain user-agent strings with outdated browser 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 three years	CAPTCHA End of Life more than two years
Chrome Version	<95	<105
Firefox Version	<95	<105
Safari Version	<13	<14
Internet Explorer Version	<11	<11

4. Threat Reduction: Proxies

The use of proxy services by malicious bots to obscure their activities is on the rise, as attackers employ these services to simulate legitimate user behavior. By leveraging IP rotation from bulk IP services, they can mask their true origins, complicating detection efforts. A strategic approach to mitigating this threat involves restricting access from known bulk IP data centers, significantly reducing the potential for botnet traffic to infiltrate your network. Notable sources of such proxy-based attacks include data centers and cloud service providers, such as Host Europe GmbH, Dedibox SAS, Digital Ocean, OVH SAS, and Choopa, LLC. Implementing access controls and monitoring for traffic originating from these entities can enhance your security posture by preemptively identifying and blocking bot-generated traffic, thereby minimizing the risk associated with these proxy-enabled attacks.

5. Threat Reduction: Automation

Modern tools like Puppeteer, Selenium, and WebDriver are often misused by attackers to imitate human actions online, enabling them to carry out harmful activities such as bulk account registrations and data theft. Distinguishing these malicious efforts from legitimate traffic requires implementing detection strategies for signs of automation, such as unnaturally fast interactions or abnormal browsing patterns. By honing in on these behaviors, organizations can effectively spot and stop automated attacks, safeguarding genuine user interactions.

6. Evaluate Traffic

A. Identifying bot traffic without explicit indicators poses a challenge, yet specific patterns often hint at their presence. High bounce rates and low conversion rates can be telltale signs of non-human traffic. Additionally, sudden unexplained spikes in traffic or an unusually high number of requests targeting a specific URL frequently signal bot activity. Monitoring for these anomalies enables organizations to flag potential bot traffic, facilitating further investigation and appropriate response measures to mitigate unwelcome interference.

B. The sudden surge in traffic to a particular endpoint might indicate bots targeting a specific event or operation. To assess whether this spike is bot-driven, analyze the source of this increased traffic. Look for patterns such as a single IP address, an ISP, or a specific URL generating traffic levels significantly above the norm. Identifying these sources can provide clear evidence of bot activity, enabling you

to take targeted action. For example, if traffic predominantly originates from a single IP or a narrow range of IPs, it's a strong indicator of automated access attempts. Such insights are crucial for deploying effective countermeasures against bot attacks, ensuring your digital assets remain protected.

7. Monitor Traffic

A.   Define your failed login attempt baseline on login pages, 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.

B.   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.

8. Awareness

Maintaining vigilance regarding global data breaches and leaks is essential. The simplicity with which attackers can purchase credential dumps from these breaches or rent bot infrastructure to automate attacks elevates the threat to a tangible risk. Bots frequently exploit freshly compromised credentials to conduct stuffing attacks and account takeovers (ATO) since these credentials are more likely to remain active. This tactic significantly raises the odds of successfully breaching user accounts on your platform. Staying informed about such breaches and understanding their implications can help you proactively strengthen your defenses, reducing the likelihood of your site becoming a target for these automated threats.

9. Evaluate Bot Protection Solutions

Evaluating bot protection solutions is crucial as the landscape of bot attacks has significantly transformed. The simplistic measures once sufficient to fend off malicious bots are now ineffective. The insights gathered in this report underscore that the sophistication and adaptability of modern bots surpass previous levels, with their ease of use and effectiveness making them a favored tool among cybercriminals. These bots rapidly evolve, rendering traditional detection methods obsolete, but they also mimic human behavior more closely than ever, making it challenging to distinguish them from legitimate users. In

this environment, where attackers leverage bots for their high reward and low-risk benefits, attempting to counteract these threats single-handedly is nearly impossible.

The need for a dynamic defense strategy is more pressing than ever. It's not just about identifying malicious bots; it's about differentiating them from beneficial ones amidst their increasing complexity. A comprehensive bot prevention solution should incorporate a layered defense approach, including user behavior analysis, profiling, and fingerprinting. This strategy not only preserves the advantages of legitimate bots but also effectively filters out malicious activities. Such a nuanced approach demands the expertise of a dedicated team capable of evolving your defenses at the pace of emerging threats.

Bad Bot Use Cases

Bad Bot Problem	Definition	How it Hurts the Business	Symptoms	Targeted Industries
Price Scraping	The use of bots to illegally monitor and track pricing information, typically in order to undercut rivals and boost sales	Loss of sales to competitors that scrape your prices, undercut them and beat you in the marketplace Damaged reputation due to scraped data being used in a way that misrepresents the business's prices or products The lifetime value of customers worsens Impacts website performance	Declining conversion rates Your SEO rankings drop Unexplained website slowdowns and downtime (usually caused by aggressive scrapers)	All businesses that show pricing: • Retail • Gaming • Airlines • Travel
Content Scraping	The use of bots to extract content and data from a website	Loss of revenue due to your business's content or data being published elsewhere, leading to fewer people visiting the original site or purchasing your products or services Duplicate content damages your SEO rankings Damage to brand reputation Impacts website performance	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)*	The use of bots to gain illegal access to user accounts belonging to someone else Usually achieved using brute force login techniques such as Credential Stuffing or Credential Cracking	Direct impact on brand loyalty and reputation, negative PR Customer frustration to due account lockout, data theft or dealing with fraudulent, increasing churn Impacts website performance, availability, and reliability Risk of noncompliance with data privacy regulations Increased support and fraud costs	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

Bad Bot Problem	Definition	How it Hurts the Business	Symptoms	Targeted Industries
Account Creation *(aka Account Aggregation, New Account Fraud)*	The use of bots to automate bulk account creation. These accounts can then be misused to perform various forms of fraud, spam content, or spread propaganda	Decreased credibility of certain platforms and websites to bot accounts that are used to spam messages or amplify propaganda Loss of revenue to bots that exploit new account promotion credits (money, points, free plays) Metrics based on the number of user accounts or social media interactions that all originate from bots may lead to poor decision making	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 • Gaming • Finance
Credit Card Fraud *(aka Carding, Card Cracking)*	The use of bots to mass-verify the validity of stolen credit card numbers or guess the missing details (CVV, expiration date, etc.)	Financial losses due to the businesses' liability for any fraudulent activity that occurs on their platforms: from costly chargebacks to lost revenue due to decreased consumer trust Damaged brand reputation Damages to the fraud score of the business Increased customer service costs to process fraudulent chargebacks Noncompliance with data privacy regulations (PCI-DSS, GDPR, etc.)	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 • Finance • Gaming
Denial-of-Service	The use of bots to overwhelm a website with requests, leading to an exhaustion of resources such as file system, memory, processes, threads, CPU, and human or financial resources	Slows the website performance causing brownouts or downtime Lost revenue from the unavailability of websites Damaged brand reputation Potential customer churn	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 and Abuse	The use of bots to automate the enumeration of potential gift card numbers against balance checking pages to steal gift card balances	Similary to credit card fraud, gift card fraud leads to fininaial losses due to bots that steal money from gift cards Increased customer service costs to process fraudulent chargebacks Poor customer reputation and loss of future sales Damaged brand reputation	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

Bad Bot Problem	Definition	How it Hurts the Business	Symptoms	Targeted Industries
Denial of Inventory	The use of bots to hold items in shopping carts without ever actually completing the purchase, thus denying them from legitimate consumers	Loss of revenue from unsold items that are held in shopping carts by bots Lower conversion rates Increased cart abandonment rates 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 complaints about lack of availability of inventory	Businesses offering scarce or time-sensitive items: • Airlines • Tickets • Retail • Healthcare
Scalping	The use of bots to gain an unfair advantage over legitimate consumers and obtain limited-availability and/or preferred goods/services	Damaged customer reputation Slows the website performance causing brownouts or downtime, leading to loss of revenue Lower lifetime value (LTV), because a bot doesn't regularly come back for additional items Lower average basket value (ABV), because bots target a single product as opposed to legitimate consumers who tend to purchase additional items	Unexplained website slowdowns and downtime (usually caused by aggressive scalping bots) Decrease in conversion rates Increase in customer complaints about lack of availability of inventory	Similar to Denial of Inventory: • Airlines • Tickets • Retail e.g. sneakers, consoles, computer hardware, limited edition items. • Healthcare
Seat Spinning	The use of bots to hold flight seats without making a payment, often up to 24 hours	Loss of revenue for unsold seats Reputation damage because legitimate consumers cannot book desired flights	As departure time approaches, seemingly fully booked flights are suddenly showing increasing numbers of empty seats	Airlines

Bad Bots by Industry

Industry	What Businesses are Included?	What Bad Bots do?
Automotive	Car Rentals, 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 Targeting Apis, 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	Streaming Services, Ticketing Platforms, Production Companies, Venues	Account Takeover, Price Scraping, Inventory Scraping, Scalping
Financial Services	Banking, Insurance, Investments, Cryptocurrency	Account Takeover, Carding, Card Cracking, Custom Content Scraping
Food & Groceries	Food Delivery Services, Online Grocery Shopping, Food & Beverage Brand Sites	Credit Card Fraud, Gift Card Fraud, Account Takeover
Gambling	Online Gaming, Casinos, Sport Betting	Account Takeover, Odds Scraping, Account Creation For Promotion Abuse
Government	Law & Government Websites, Citizen Services, States, Municipalities, Metropolitans	Account Takeover, Data Scraping Of Business Registrations Listings, Voter Registration, Appointment Scraping and Scheduling
Healthcare	Health Services, Pharmacies	Account Takeover, Content Scraping, "Helpful" Bots That Scrape For Appointment Availability
Lifestyle	Lifestyle Magazines, Blogs	Proprietary Content Scraping
Marketing	Marketing Agencies, Advertising Agencies	Proprietary Content Scraping, Ad Fraud, Denial-Of-Service, Skewing
News	News Sites, Online Magazines	Proprietary Content Scraping, Ad Fraud, Comment Spam
Retail	Ecommerce, Marketplaces, Classifieds	Account Takeover, Scalping, Denial of Inventory, Credit Card Fraud, Gift Card Fraud, Data and Price Scraping, Analytics Skewing
Community & Society	Nonprofits, Faith and Beliefs, Romance and Relationships, Online Communities, LGBTQ, Genealogy	Content and 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, Seat Spinning

The State of API Security in 2024

KEY FINDING

71% of all web traffic today is API related.

## The Role of Client-Side Protection in Modern Application Security

KEY FINDING

On average, modern web applications load 209 client-side resources at any time.

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 and observe trends consistently.

Least attacks   Most attacks
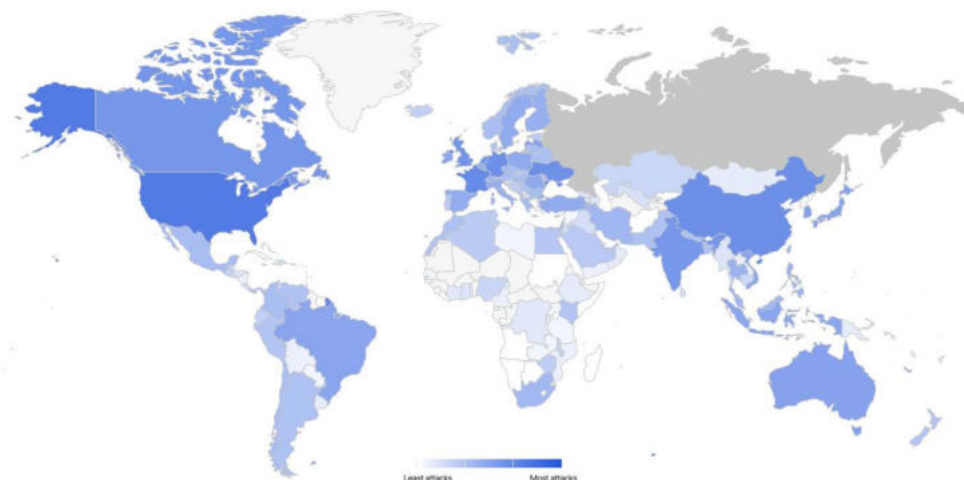
About Imperva Application Security

Imperva is the cybersecurity leader that helps organizations protect critical applications, APIs, and data anywhere, at scale, and with the highest ROI. The Imperva Application Security Platform stops the most advanced attacks with the highest efficacy while minimizing false positives. Its high efficiency enables organizations to quickly onboard, protecting their assets at scale. With the help of the Imperva Threat Research Team and our global intelligence community, we stay ahead of the evolving threat landscape, seamlessly integrating the latest security, privacy, and compliance expertise into our solutions.

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

- **On-Prem and Cloud Web Application Firewall (WAF) solutions** for blocking the most critical web application security risks.

- **API Security** for continuous protection of all APIs using deep discovery and classification.

- **Advanced Bot Protection** for safeguarding websites, mobile applications, and APIs against today's most sophisticated automated threats.

- **Client-Side Protection** for safeguarding websites against client-side attacks and streamlining regulatory compliance with PCI DSS 4.0.

- **DDoS protection** for websites, networks, and DNS to ensure business continuity with guaranteed uptime.

- **Runtime Application Self-Protection (RASP)** for security by default against known and zero-day vulnerabilities.

- **Content Delivery Network** for securely delivering applications worldwide with superior speed and performance.

Start your Application Security Free Trial today to protect your applications from Bad Bots.