

**imperva**

**2023**

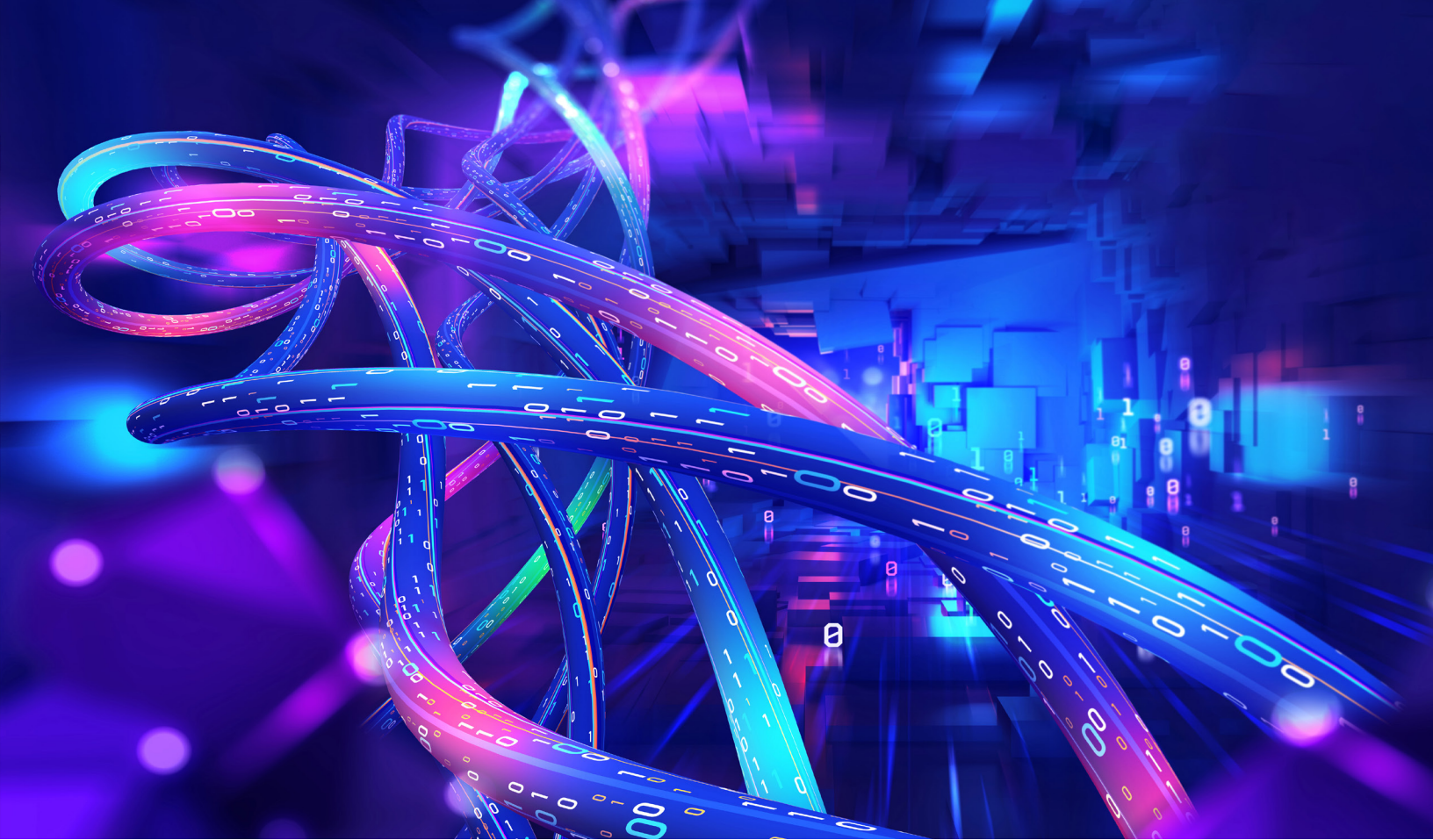
# Bad Bot Report



---

# Table of Contents

|  |           |
|--|-----------|
| <b>01 About the Imperva Bad Bot Report</b>                           | <b>03</b> |
| <b>02 Definitions</b>  | <b>04</b> |
| <b>03 Executive Summary</b>  | <b>05</b> |
| <b>04 Account takeover attacks continue to be a menace</b>           | <b>09</b> |
| <b>05 The bad bot landscape</b>                                      | <b>11</b> |
| • Bad bot traffic by industry  | 11        |
| • Bad bot sophistication by industry                                 | 15        |
| • Most targeted industries by bot attacks                            | 16        |
| • Bad bots appreciate the privacy offered by certain mobile browsers | 17        |
| • The rise of mobile user agents continues                           | 18        |
| • Data Centers regain popularity                                     | 19        |
| • A varied mix of all ISP types among the top 10                     | 19        |
| • Mobile and residential among the top bot-originating ISPs          | 20        |
| • Bad bots across the globe  | 21        |
| • The United States and Australia were the most targeted countries   | 22        |
| <b>06 A 10-Year Evolution of Malicious Automation</b>                | <b>23</b> |
| <b>07 Recommendations</b>  | <b>35</b> |
| <b>08 Appendix</b>   | <b>37</b> |
| • Bad bot use cases  | 37        |
| • Bad bots by industry   | 41        |
| <b>09 Imperva Threat Research</b>                                    | <b>43</b> |
| <b>10 About Imperva Application Security</b>                         | <b>44</b> |



---

## About the Imperva Bad Bot Report

**This report focuses on bad bot activity at the application layer (layer 7 of the OSI model). These are entirely different from volumetric DDoS attacks, the latter of which manipulate lower-level network protocols.**

The 10<sup>th</sup> annual Imperva Bad Bot Report is a threat research report that analyzes and investigates the automated attacks occurring daily, sneaking past traditional detection methods and wreaking havoc on the internet. It is based on data collected from the company's global network throughout 2022, which includes 6 trillion blocked bad bot requests, anonymized across thousands of domains.

This 10th edition of the report not only delves into the latest trends and statistics surrounding bad bots but also provides a retrospective look at bots over the past decade. In addition, this report offers meaningful information and guidance about the nature and impact of bots to help organizations better understand the potential risks of bot traffic when not properly managed.

Bad bots interact with applications like legitimate users would, making them harder to detect and block. They abuse business logic by exploiting the way a business operates, rather than exploiting technical vulnerabilities. They enable high-speed abuse, misuse, and attacks on 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, scalping, digital ad fraud, denial of service, spam, transaction fraud, and more. They can consume bandwidth, slow down servers, and steal sensitive data, leading to financial losses and damage to a company's reputation.



---

# Definitions

Before we dive deep into the data, let's first define a few of the key terms that will be used 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 tasks like scraping a website for data.

## 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. An example of this is bots that perform credential stuffing to take over user accounts – one of the most prominent bot attacks. The Open Web Application Security Project (OWASP) provides a comprehensive list of 21 different bot attacks in its Automated Threat Handbook<sup>1</sup>.

## What is the difference between good and bad bots?

Not all bots are created equal; there are good bots on the internet, too. These serve useful functions such as indexing websites for search engines or monitoring website performance. For example, search engine crawlers such as Googlebot and Bingbot help create and maintain a searchable index of web pages. Through their indexing, these bots help people match their queries with the most relevant sets of websites. They are crucial for online businesses because they ensure that their websites and their products or services can be easily found and reached by prospective customers.

## Even good bots can be a cause for concern

Good bots can skew web analytics reports, making some pages appear more popular than they actually are. For example, if you advertise on your website, good bots can generate an impression, but that ad click never converts into the sales funnel. This results in lower performance for advertisers. It can also lead to skewed marketing analytics and incorrect decision-making based on them. Therefore, being able to intelligently distinguish between traffic generated by legitimate human users, good bots, and bad bots is crucial for making informed business decisions.

## Bad bot classification

Imperva has 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** – Emulating 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 Bad Bots

Technological advancements in bad bot evasion techniques in recent years have further thinned the line between moderate and advanced bad bots. For this reason, we are offering another perspective on bad bot traffic analysis by grouping both Moderate and Advanced bots together. As their name suggests, Evasive bots use the latest evasion techniques, including cycling through random IPs, entering through anonymous proxies, changing their identities, mimicking human behavior, delaying requests, defeating CAPTCHA challenges, and more. They use a mix of sophisticated technologies and tactics to evade detection while maintaining persistence on target sites. They often choose a "low and slow" approach, which enables 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.

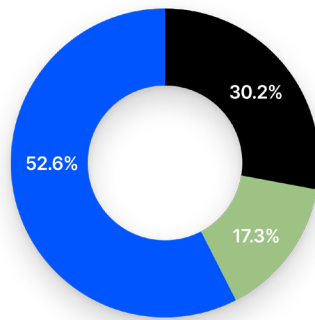
---

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

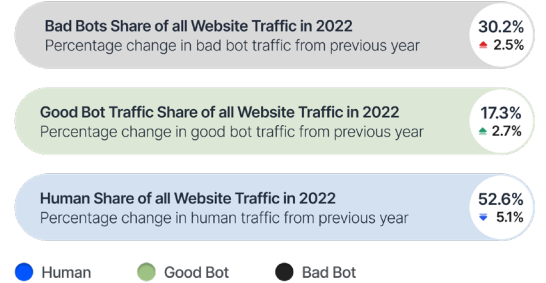
# Executive Summary

## Nearly half of the internet traffic in 2022 was bots

Of all internet traffic in 2022, 47.4% was automated traffic, also commonly referred to as bots. Compared to 42.3% in 2021, that is a 5.1% increase. Of that automated traffic, 30.2% were bad bots, a 2.5% increase from 27.7% in 2021. Good bots are on the rise too, accounting for 17.3% compared to 14.6% in 2021. Alarmingly, the percentage of human traffic continues its downward trend, from 57.7% in 2021 to 52.6% in 2022 – a 5.1% decrease. Of all the attacks recorded by Imperva in the past year, 27% were bad bots that abuse business logic and 26% were other types of automated threats.

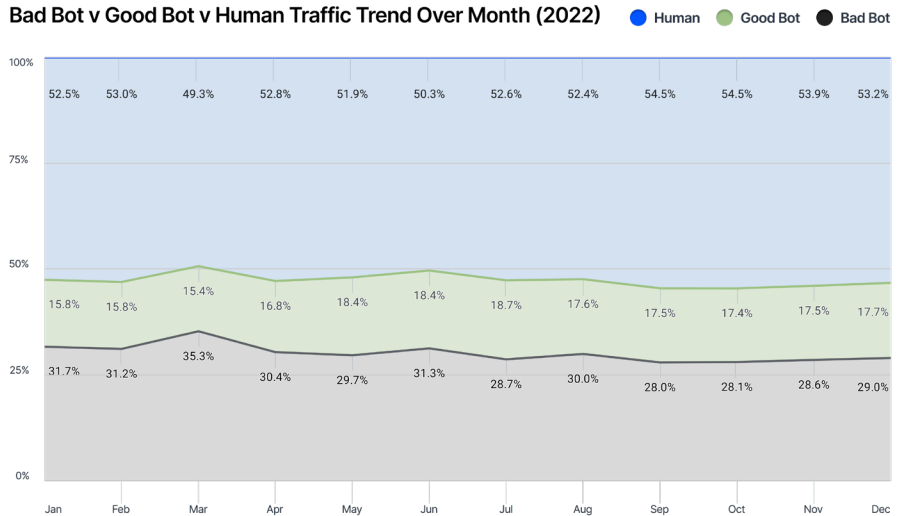


### Bad Bot v Good Bot v Human Traffic 2022



The following chart represents a monthly trend analysis of the profile of internet traffic. We can see that the trend has been steadily consistent throughout the year, barring some more noticeable changes in March and June. In March, specifically, human traffic levels were just slightly less than half of all internet traffic (49.3%), as bad bot traffic peaked (35.3%). This could be attributed to an increase in bot attacks recorded by Imperva during the same period.

### Bad Bot v Good Bot v Human Traffic Trend Over Month (2022)



## Looking back at a decade of fighting bad bots

2023 marks the 10th anniversary of the Bad Bot Report – a good opportunity to look back at how the profile of internet traffic has changed throughout the past decade.

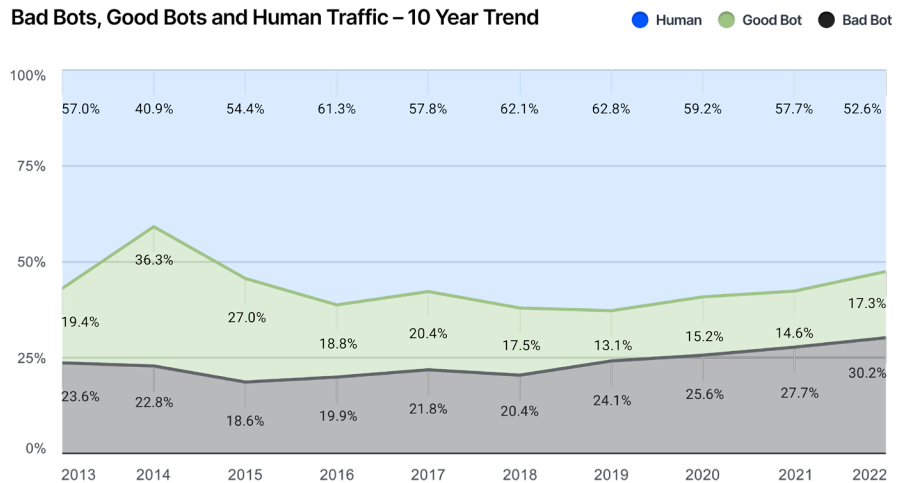
In 2013, the profile of internet traffic somewhat resembled that of recent years, with bad bots accounting for 23.6% of traffic, good bots accounting for 19.4%, and human traffic for 57%.

2014 was an interesting year in the sense that we saw a significant move in good bot traffic, which grew from 20.98% to 36.32%, potentially due in part to more aggressive indexing by Bing and upstart search engines during that year.

2015 marked the lowest point for bad bot traffic, as human traffic increased to 54.4%. This can be explained by the significant influx of new internet users, especially from China, India, and Indonesia. Additionally, bot operators were opting for quality, instead of quantity, developing more advanced bots that can achieve more with fewer requests.

Other low points for bad bot traffic were in 2016 and 2018, as they accounted for 19.9% and 20.4%, respectively. Since then, however, bad bot traffic levels have been on a 4-year upward trend, going from 24.1% in 2019 to an all-time high of 30.2% of all internet traffic in 2022.

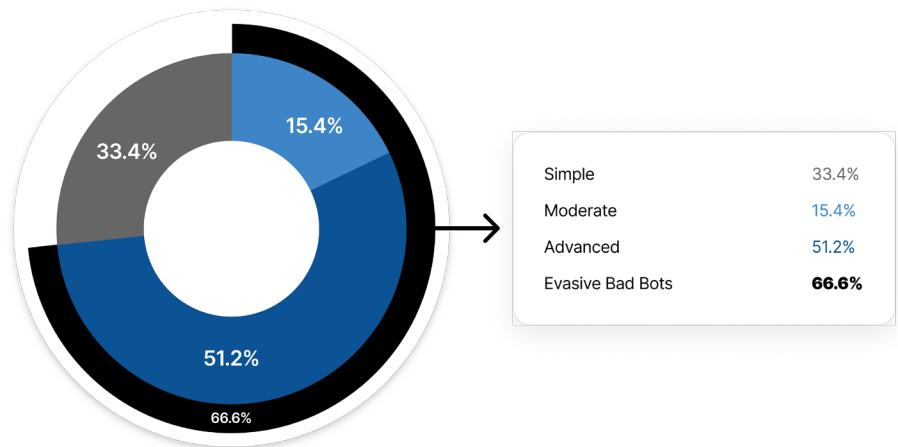
Bad Bots, Good Bots and Human Traffic – 10 Year Trend



## Bad bots are more advanced than ever

As bad bot evasion techniques become increasingly sophisticated, we are observing a fascinating trend, where advanced bad bot levels (51.2%) are growing at the expense of moderate ones (15.4%). Simple bad bot levels have remained similar, at about a third (33.4%) of all bad bot traffic. Because moderate and advanced bad bots represent the more “self-conscious” bots that go to greater lengths to hide their true identity, we often group them and refer to them as evasive bad bots. In 2022, these evasive bad bots accounted for 66.6% of all bad bot traffic – a slight increase from the previous year (65.5%). While the increase isn’t substantial, it is the makeup of evasive bad bots that is alarming, with advanced bad bot levels essentially doubling.

Bad Bot Sophistication Levels 2022



## APIs are more susceptible to bad bots

Of all the attacks that targeted APIs this past year, 17% were bad bots that abuse business logic and 21% were other types of automated threats. A business logic attack is an attack that targets flaws in the design and implementation of an application. Such flaws can be exploited by attackers to manipulate legitimate functionality and achieve various types of malicious goals such as stealing sensitive data and gaining illegal access to user accounts. APIs are an essential part of modern software development. However, if not adequately secured with business logic in mind, they can be highly susceptible to bad bots that exploit business logic vulnerabilities to wreak havoc.

Imperva has recently mitigated two types of bot attacks that abused business logic on APIs. The first was when an airline had its search API heavily scraped by bots for flight information, resulting in over \$500K in charges per month for API requests. The second was an online bank that had its login API targeted by massive account takeover attacks of over 2 million requests, causing a large number of account lockouts and online fraud occurring in hacked accounts. In both scenarios, the attacks have been immediately mitigated once onboarded to Imperva. And these are just a few of the ways in which bots can abuse business logic on APIs, resulting in significant damage to businesses’ bottom line.

# Executive Summary

## Bad bots affect all industries

Bad bots are a cross-industry, cross-functional problem. Their ability to perform various malicious actions at a capacity and velocity that is downright impossible for a normal human being makes them an ideal tool for high-speed abuse, misuse, and attacks. And while some bad bot use cases, like content scraping and account takeover, are shared across various industries, there are also industry-specific use cases, such as scalping that usually affect online retailers and entertainment (ticketing).

| Largest Share of Bad Bot Traffic By Industry in 2022 |                     |       |
|--|---------------------|-------|
| 1  | Gaming              | 58.7% |
| 2  | Telecom & ISPs      | 47.7% |
| 3  | Community & Society | 41.1% |
| 4  | Computing & IT      | 40.0% |
| 5  | Business Services   | 38.0% |

| Largest Share of Advanced Bad Bot Traffic By Industry in 2022 |                    |       |
|---|--------------------|-------|
| 1   | Law & Government   | 89.0% |
| 2   | Travel             | 63.4% |
| 3   | Telecom & ISPs     | 60.5% |
| 4   | Retail             | 51.9% |
| 5   | Financial Services | 45.8% |

## Mobile remains a popular choice for bad bot operators

The popularity of mobile browsers among bad bot operators continues to increase, as 39.1% of bad bots attempt to evade detection by disguising themselves as one. Mobile ISPs retain their popularity as well, with 26.9% of attacks launched from them. The share of bad bots that were launched from AWS increased from 7.95% in 2021 to 17.4% in 2022.

Bad bots report as mobile user agents (Mobile Safari, Mobile Chrome etc) **39.1%**

Bad bots launched from mobile ISPs **26.9%**

Bad bots using Amazon ISP **17.4%**

## Bad bots across the globe

While remaining at the top of the list of most attacked countries by bad bots, the US has slightly dropped, from 43.1% of attacks in 2021 to 41.8% in 2022. Australia remained second, increasing to 16.4%, up from 6.8% in 2021.



### Top 5 Most Targeted Countries by Bad Bots

 1 United States 41.8%

 2 Australia 16.4%

 3 United Kingdom 6.8%

 4 France 3.6%

 5 Germany 2.8%



---

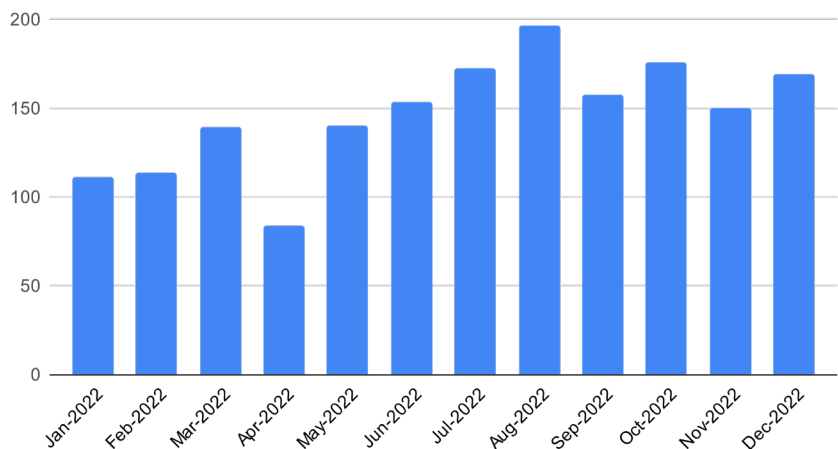
## Account takeover attacks continue to be a menace

The growth in account takeover attacks (ATO) continues, fueled by data breaches, new incentives, and an ongoing commoditization of acquiring bot infrastructure.

There were more than 4,100 publicly disclosed data breaches in 2022 alone, which equates to approximately 22 billion records being exposed<sup>2</sup>. There is often a correlation between data breaches and account takeover attacks, as attackers attempt to utilize leaked credentials from recently disclosed data breaches before users have time to realize their data has been exposed.

An example of such correlation could be seen during Q3 2022, as a reported 70% rise in data breaches<sup>3</sup> across the globe corresponded to a 40% increase in account takeover attacks that were recorded by Imperva at the exact same time.

**Account Takeover Incidents Over Month**



## Account takeover targeting APIs

We are seeing an increase in the targeting of APIs by account takeover attacks, with 35% of attacks targeting APIs specifically. An Application Programming Interface (API) is software that serves as a way for two or more applications to talk to each other. They are commonly used by mobile apps, web applications, and Internet of Things (IoT) devices to communicate with servers and databases. The abundance of APIs is one reason why they have become a prime target for account takeover attacks, but there is more to it. APIs are simpler to attack: they rely on the use of a token as a form of authentication and thus require no need for parsing. Instead, these tokens and other forms of authentication can be intercepted or stolen by attackers and then be used to gain unauthorized access to the API and the associated account or data. Because APIs are often called programmatically, it means that an attacker can more easily automate the process of attempting to take over an account without raising any alarms. The process is also faster since there is no need for browser automation.

---

<sup>2</sup> <https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022>

<sup>3</sup> <https://www.infosecurity-magazine.com/news/data-breaches-rise-by-70-q3-2022/>

# Account takeover attacks continue to be a menace

## Account takeover attacks by the numbers

|             |   |
|-------------|---|
| <b>155%</b> | Growth in account takeover attacks between 2021 and 2022  |
| <b>15%</b>  | Percentage of account takeover attempts out of all logins |
| <b>35%</b>  | Percentage of account takeover attacks that targeted APIs |

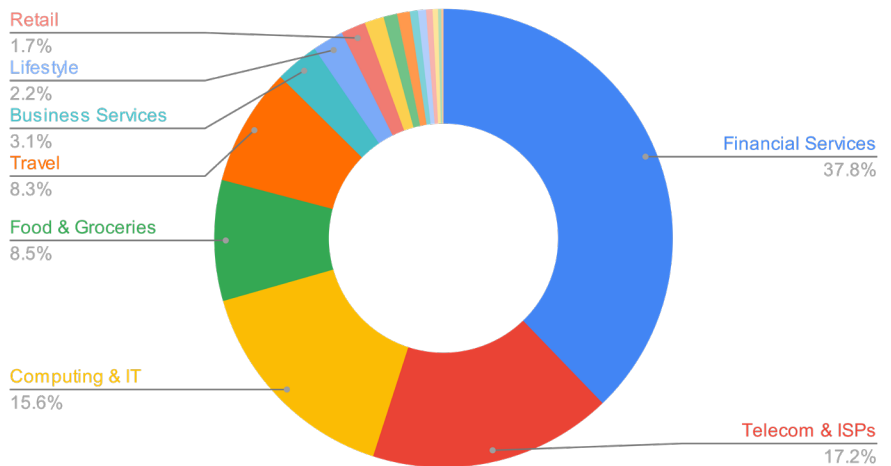
| Industries with the highest ATO ratio of all logins |              |
|---|--------------|
| Sports  | <b>37.7%</b> |
| Automotive  | <b>30.4%</b> |
| Travel  | <b>24.2%</b> |
| Computing & IT                                      | <b>20.4%</b> |
| Healthcare  | <b>20.4%</b> |
| Telecom & ISPs                                      | <b>19.6%</b> |

| Most targeted countries by ATO attacks |  |
|--|--|
| United States                          |  |
| Netherlands                            |  |
| Brazil                                 |  |
| Mexico                                 |  |
| Puerto Rico                            |  |
| Italy                                  |  |

## Most-attacked industries

The following chart illustrates what industries experienced the largest volume of account takeover attacks in 2022. Financial Services were heavily targeted, accounting for 37.8% of all ATO attacks, followed by Telecom & ISPs (17.2%), Computing & IT (15.6%), and Food & Groceries (8.5%).

Account Takeover Attacks by Industry



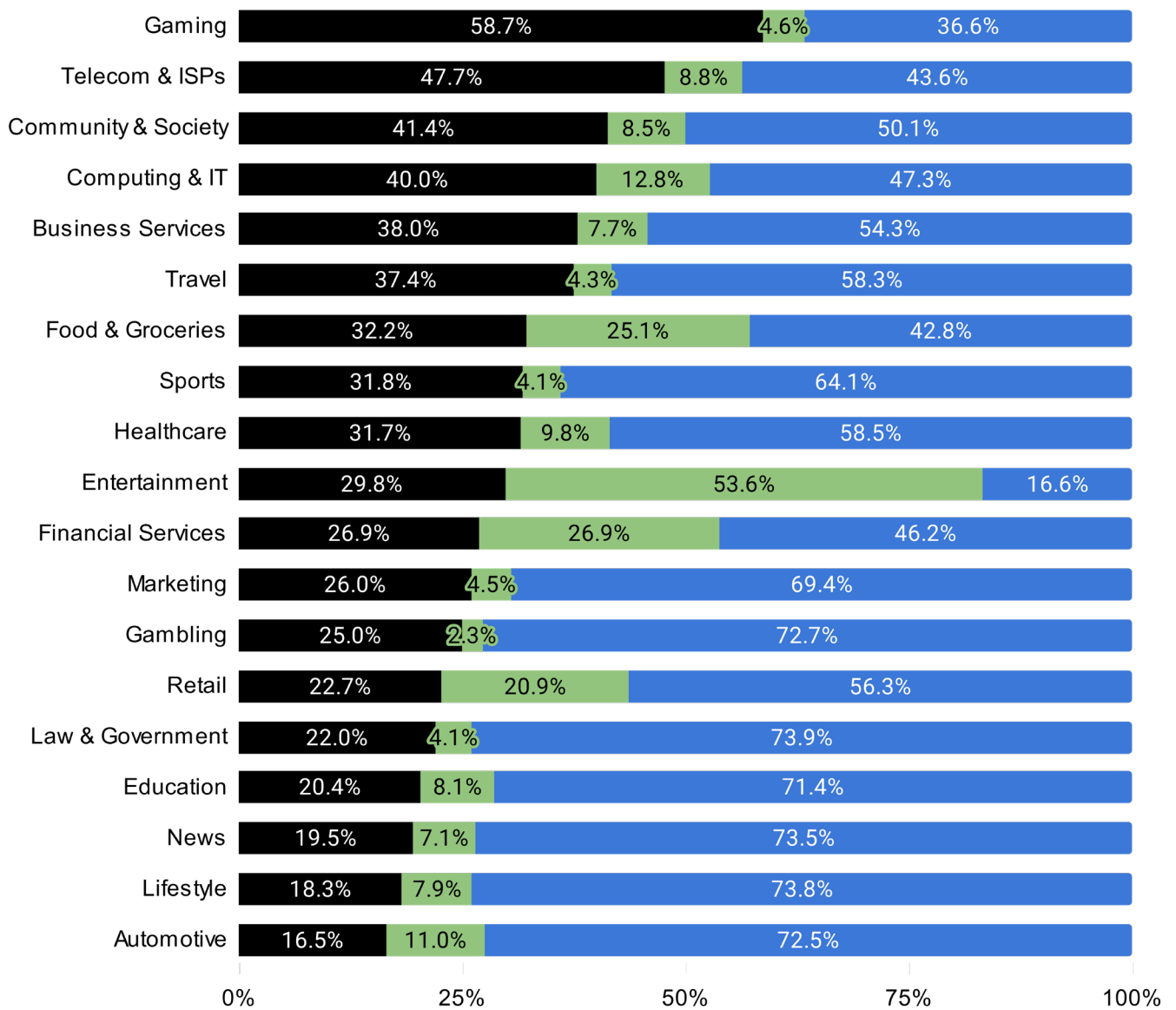
# The bad bot landscape

## Bad bot traffic by industry

The following chart illustrates what industries experienced the largest volume of Account Takeover attacks in 2022. Financial Services were heavily targeted, accounting for 37.8% of all ATO attacks, followed by Telecom & ISPs (17.2%), Computing & IT (15.6%), and Food & Groceries (8.5%).

## Bad Bot v Good Bot v Human Traffic 2022 - Industry Breakdown

● Human ● Good Bot ● Bad Bot



---

## The bad bot landscape



**GAMING** websites had a significant proportion of their traffic (58.7%) originating from bad bots. Bots can cause trouble for online gaming and video games by taking over user accounts, generating fake accounts for the exploitation of benefits, and cheating. They can perform actions difficult or impossible for human players, like high-speed interactions with a game to beat human players or nonstop farming of virtual currency, items, or experience points (XP). This disrupts the balance of play in online games, making them unenjoyable for legitimate, human players who leave the game, leading to a decline in active player numbers and revenue loss.



**TELECOM & ISPs** had a slight increase in traffic originating from bad bots, up from 46.9% in 2021 to 47.7% in 2022. This sector includes mobile ISPs, residential ISPs, hosting providers, and more. Bad bots target this industry with various malicious activities such as scraping sensitive customer data and brute force login attacks to take over user accounts. Since this sector is highly dependent on availability and sensitive to downtime, bad bots target it with an overwhelming number of requests, masquerading as legitimate users, in an attempt to overwhelm their infrastructure and hamper services. Bot traffic may also skew website analytics, leading to misguided decision-making.



**COMMUNITY & SOCIETY** websites had bad bots accounting for 41.4% of their traffic. One of the most common bad bot problems in the industry is spam bots, also known as Fake News Spam and Comment Spam. These bad bots spread fake news, amplify propaganda, and hide malicious content like malware inside clickbait links. This sector also includes many nonprofit organizations that accept donations on their websites. Bots use their donation pages to test stolen credit card numbers, causing great trouble and a financial burden many nonprofits cannot afford.



**COMPUTING & IT** saw 40% of their traffic originating from bad bots. The negative impact of bad bots on the industry ranges from causing technical problems to committing fraud and posing security threats. A common way bad bots are targeting this sector is with Distributed Denial of Service (DDoS) attacks, where a large number of bots overwhelm the servers of a website with requests. Bots are also used to scrape sensitive data, such as login credentials and personal information, leading to potential data breaches and identity theft. Other potential use cases include vulnerability scanning and click fraud, which leads to skewed metrics and revenue losses.

---

# The bad bot landscape



**TRAVEL** websites are returning to pre-pandemic popularity among bad bot operators. Following a two-year period of decreased bad bot activity, this year the sector had 37.4% of all web traffic to travel sites originating from bad bots. The travel industry suffers from some of 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 cause site slowdowns and downtime — leading to customer dissatisfaction during disruptions. Airlines specifically suffer from ATO issues as bad bot operators attempt to get into user accounts and steal accumulated air mile balances.



**FOOD & GROCERIES** websites experienced 32.3% of their traffic originating from bad bots. This category includes sites related to food delivery services and online grocery stores. The most common bad bot use case affecting this sector is price scraping. Competing businesses deploy bad bots to scrape websites for product listings and pricing, using that information to undercut pricing and even copy product listings, leading to a loss of business and revenue. However, not all price scraping is malicious – search engines and price comparison websites also scrape for prices and product availability. This might explain why 25.1% of traffic to food & groceries websites was from good bots. These bots can potentially benefit businesses, by driving traffic and exposure, leading to increased sales and brand awareness. However, that makes it crucial for businesses in this sector to not only be able to differentiate between human and bot traffic but also to determine the nature of that bot traffic. These sites are often targeted by bots performing Account Takeovers with criminals seeking the various forms of payment available within customer accounts – stored credit card numbers, loyalty points, and gift card balances. Another common form of business logic abuse by bad bots is account creation. Bad bots automate mass account creation, often exploiting new user benefits or committing fraudulent purchases using credit cards. Price scraping by competitors remains a common threat.



**RETAIL** websites saw 22.7% of their traffic originating from bad bots. Like food & groceries websites, online retailers experienced a high volume of good bot traffic (20.9%), due to the prevalence of price scraping by competitors and search engines or price comparison websites. There are several factors contributing to the slightly lower rate of bad bot traffic compared to previous years. First, the return to popularity of in-store shopping. Second, there were fewer cases of extremely high-demand products with limited stock (e.g. gaming consoles and GPUs). Lastly, the global economy is swaying between inflation and a potential recession, directly affecting sales. 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 consistently faces.



---

# The bad bot landscape



**HEALTHCARE** websites experienced 31.7% of traffic originating from bad bots. These bots can cause healthcare data breaches, taking over user accounts to access their medical records or scraping sensitive health information, such as patient records, medical history, and insurance information. This data can later be sold on the dark web for profit or used for fraudulent activities. Another risk posed by bad bots in healthcare is overloading their systems through Distributed Denial of Service (DDoS) attacks, which overload healthcare websites and systems, making it difficult for patients and healthcare providers to access the information and services they need. At the time of writing these lines, Imperva has monitored an increase in DDoS attacks on US healthcare organizations by the Pro-Russian hacktivist group Killnet<sup>4</sup>. This can be highly disruptive to telemedicine services, hindering communication between patients and providers. Bots can also spread misinformation and spam about healthcare, potentially leading to misdiagnosis, mistreatment, and other harmful outcomes. For example, in the early days of the pandemic, the concern over the Coronavirus was exploited to increase the online popularity of spam campaigns designed to spread fake news and drive unsuspecting users to dubious online drug stores<sup>5</sup>. Overall, bot activity on healthcare websites can be disruptive and costly, draining resources, causing downtime, and contributing to security breaches that require time and money to remediate.



**FINANCIAL SERVICES** websites had bad bots make up 26.9% of their traffic. The biggest threat to this sector is account takeover attacks, where bad bots attempt illegal access to user accounts through various brute-force login techniques, such as credential stuffing or credential cracking. Other popular threats include credit card fraud and custom content theft, such as frequently changing interest rates. Recently, a new type of bot has been targeting this sector: Arbitrage Bots. These bots target cryptocurrency exchanges and NFT marketplaces, leveraging web scraping to identify and exploit imbalances in the pricing between different exchanges and marketplaces. They enable operators to trade crypto and NFTs from one exchange or marketplace to another, capitalizing on pricing differences between the same coin or pairs on different exchanges to make a profit.

---

<sup>4</sup> <https://www.imperva.com/blog/hospitals-hit-by-ddos-attacks/>

<sup>5</sup> <https://www.imperva.com/blog/concern-over-coronavirus-leading-to-global-spread-of-fake-pharmacy-spam/>

# The bad bot landscape

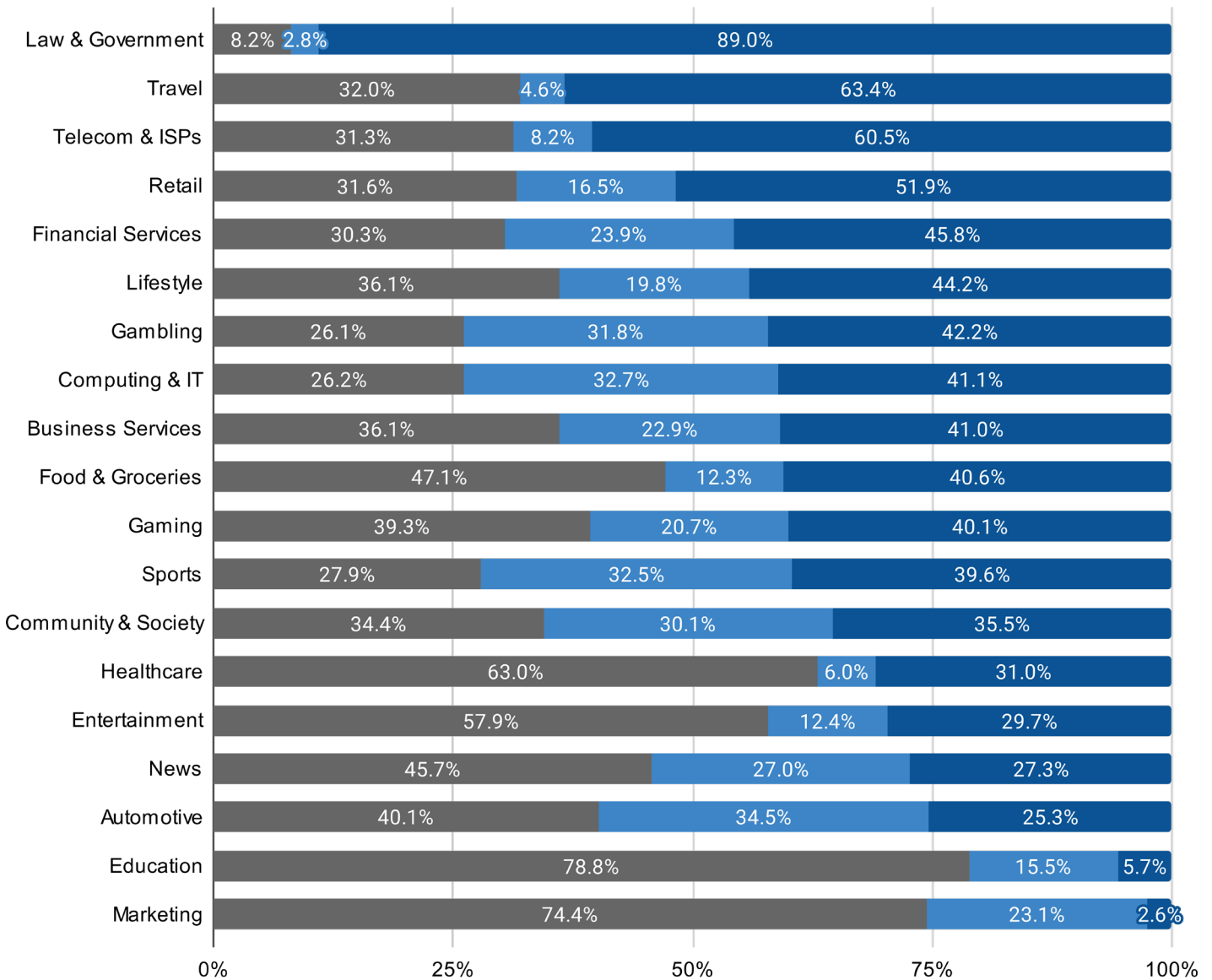
## Bad bot sophistication by industry

To better understand the bad bot risks each industry faced this year, the following chart offers a breakdown of 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 can achieve their goals while performing fewer requests than simpler bad bots.

### Bad Bot Sophistication in 2022 - by Industry

● Simple ● Moderate ● Advanced

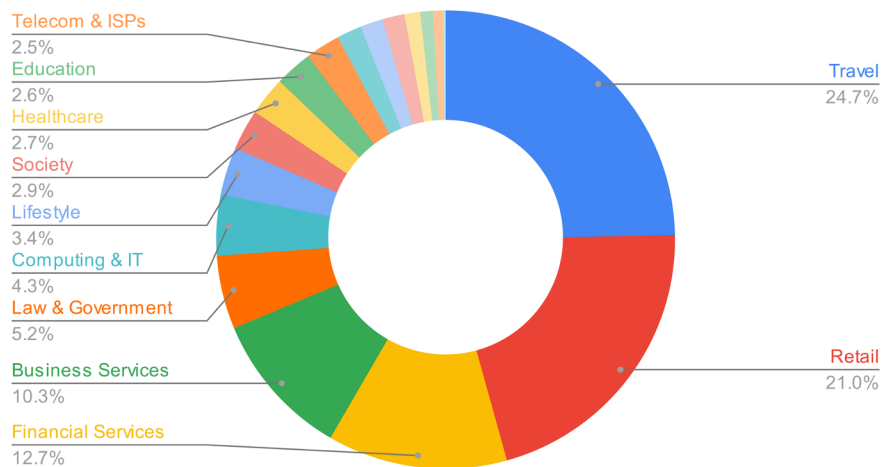


# The bad bot landscape

## Most targeted industries by bot attacks

While the breakdown of the traffic profile for each industry reveals the ratio of bot traffic out of all traffic, the distribution of bot attacks across the industries provides a different perspective. It reveals which industries were targeted by the most bot attacks, attempting to abuse business logic and wreak havoc. The top three most targeted industries are travel, retail, and financial services. As covered earlier in this report, each of these suffers from a complex bot problem, with various bot use cases threatening their businesses. It is important to note that the fact a certain industry had a high ratio of bad bots doesn't necessarily correlate with the industry being targeted more or less than other industries. An industry can have a low ratio of bot traffic because it has seen significant numbers of human traffic throughout the year, or it has been targeted by more advanced bad bots that require fewer requests to achieve their desired outcomes.

Most Targeted Industries by Bot Attacks



# The bad bot landscape

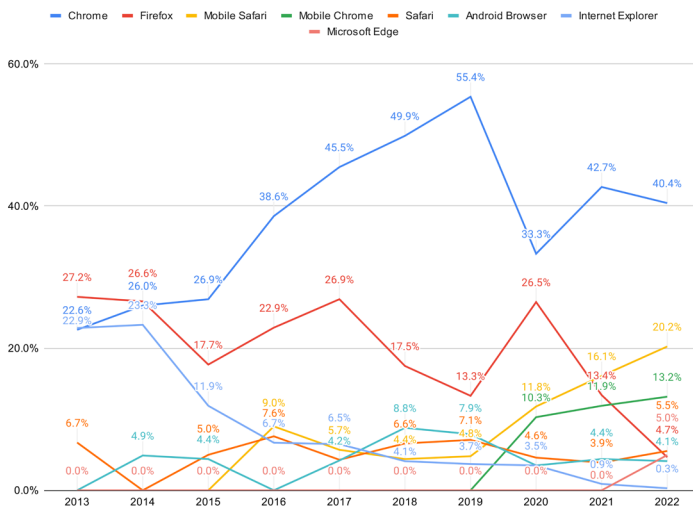
## Bad bots appreciate the privacy offered by certain mobile browsers

One of the many layers comprising bad bots' evasion techniques today is hiding their true identity by masquerading as legitimate users by reporting themselves as a web or mobile browser that's popular among human users. This is often achieved through the use of browser automation software. What started as an advanced evasion technique a decade ago is now a commodity across most, if not all, bad bots. But what's more interesting is how the trend of popularity of the different browsers among bad bots has changed over the past decade. These changes reflect both the popularity of these browsers among human users as well as other trends that aid bots in evading detection.

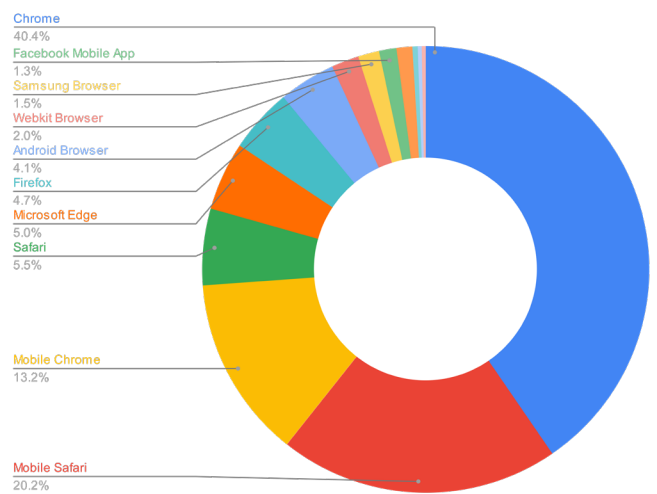
The most interesting observation is the persistence of a trend we started tracking last year – the increase in popularity of bad bots opting for Mobile Safari as their browser of choice. No less than a fifth (20.2%) of bot traffic self-reported as this browser. That is another significant jump, up from 11.8% of traffic in 2020 and 16.1% in 2021. It is now clear that the improved user privacy settings offered by this browser are being exploited by bots to mask their behavior, which makes them even harder to detect.

Bots masquerading as Chrome browsers slightly dropped in volume, from 42.7% of traffic in 2021 to 40.4% in 2022. Similar to Mobile Safari, the use of Mobile Chrome increased too, accounting for 13.2% of traffic compared to 11.9% in 2021.

Top Self Reporting Browsers by Bad Bots 2013 - 2022



Top Self Reported Browsers by Bad Bots in 2022



# The bad bot landscape

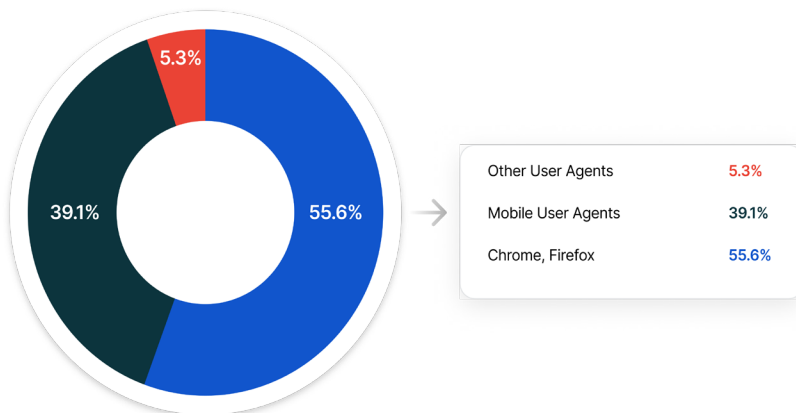
## The rise of mobile user agents continues

As of November 2022, 60.28% of all web traffic came through mobile phones<sup>6</sup>. Bot operators realize that too, which is why they choose to disguise themselves as one form or another of mobile-based user agent as part of their evasion technique. They understand that they must follow the trend of how legitimate human users are browsing the web. Furthermore, there are additional benefits to using certain mobile user agents, such as Mobile Safari and recently Mobile Chrome. The added privacy features that these browsers offer, Mobile Safari in particular, allow bad bots to better disguise themselves. Still, the majority of bad bots (55.6%) are self-reporting as either Chrome, Firefox, Safari, or Internet Explorer. However, their popularity among bad bot operators is decreasing over the past years, from 68% of traffic in 2020 to 60.9% in 2021 and 55.6% in 2022.

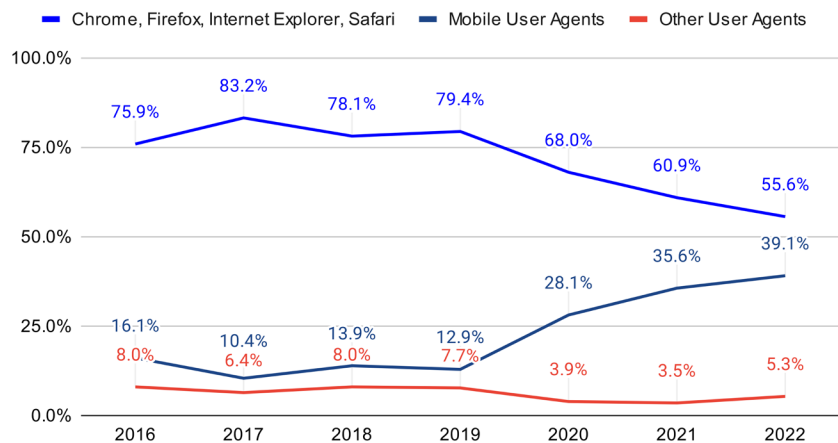
On the other hand, bad bots masquerading as mobile user agents are on a steady, upward trend: from 28.1% in 2020 to 35.6% in 2021 and 39.1% in 2022. We predict that this trend of growth in bad bots opting for mobile user agents over desktop-based ones will persist in the coming years.

The rest of the bad bot traffic, 5.3%, has reported themselves as other user agents (e.g. Google Search App or QQ and WeChat browsers).

Bad Bot Reported User Agent Types 2022



Bad Bot Reported User Agent Types 2016-2022





---

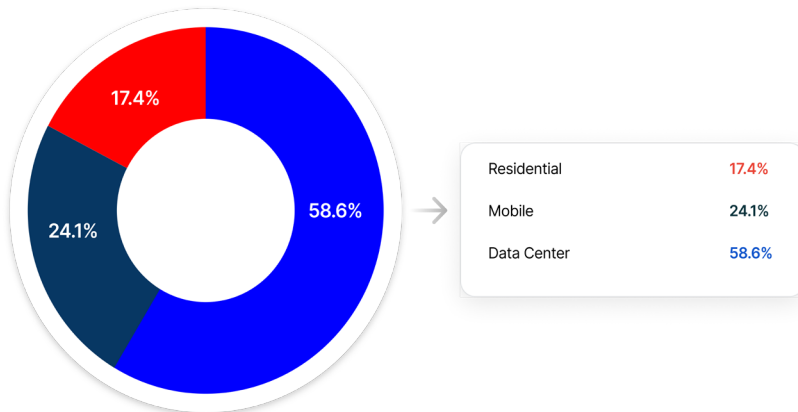
# The bad bot landscape

## Data centers regain popularity

Data centers have been the weapon of choice for a majority of bad bot traffic in previous years, but traffic originating from them has been decreasing, going from 54% in 2020 to 45.1% in 2021. This year, however, bad bots originating from data centers increased by 13.5% to 58.6% of all bad bot traffic. While the number of bad bots originating from residential ISPs decreased from 27.7% to 17.4%, we are still seeing a large number of highly sophisticated bot campaigns launched from these.

The amount of traffic originating from mobile ISPs remained similar to last year, only slightly decreasing from 27.2% of traffic in 2021 to 24.1% in 2022.

Bad Bot Traffic by ISP Type 2022



## A varied mix of all ISP types among the top 10

- The use of Amazon as an ISP has significantly risen to 17.4% (compared to 10.8% in 2020 and 7.95% in 2021). That is very close to its all-time high of 18%.
- Korea Telecom, a mobile ISP, has claimed the second spot, amounting to 5.2%.
- Telstra Internet, a residential ISP, has cracked the top 10, with 2.5% of bot traffic.
- Contabo GmbH, Digital Ocean, and OVH SAS claimed the 3rd, 4th and 9th spots.

# The bad bot landscape

## Mobile and residential among the top bot-originating ISPs

While residential and mobile ISPs remain a force to be reckoned with as a source of advanced bot attacks, this year, attackers leaned more towards data centers and hosting providers. By taking a look at the list of the top 10 bot-originating ISPs, we can see that mobile and residential ISPs are still highly popular among bad bot operators. Notice that Korea Telecom claimed the second spot and Telstra Internet sits at the fifth, meaning they had a significant proportion of bot traffic originating from them.

| Top 10 Bot Originating ISPs    |                  |
|--------------------------------|------------------|
| ISP                            | % of bot traffic |
| Amazon.com                     | 17.4%            |
| Korea Telecom                  | 5.2%             |
| Contabo GmbH                   | 2.5%             |
| Digital Ocean                  | 2.5%             |
| Telstra Internet               | 2.5%             |
| Microsoft Azure                | 1.9%             |
| Safaricom                      | 1.7%             |
| Stark Industries Solutions Ltd | 1.6%             |
| OVH SAS                        | 1.4%             |
| Maxis Communications           | 1.3%             |

| Top 10 Bot Originating Mobile ISPs |                  |
|------------------------------------|------------------|
| ISP                                | % of bot traffic |
| Korea Telecom                      | 5.2%             |
| Safaricom                          | 1.7%             |
| Maxis Communications               | 1.3%             |
| China Telecom                      | 0.8%             |
| Optus                              | 0.8%             |
| StarHub                            | 0.6%             |
| AIS Mobile                         | 0.5%             |
| T-Mobile USA                       | 0.5%             |
| EE                                 | 0.5%             |
| SK Telecom                         | 0.4%             |

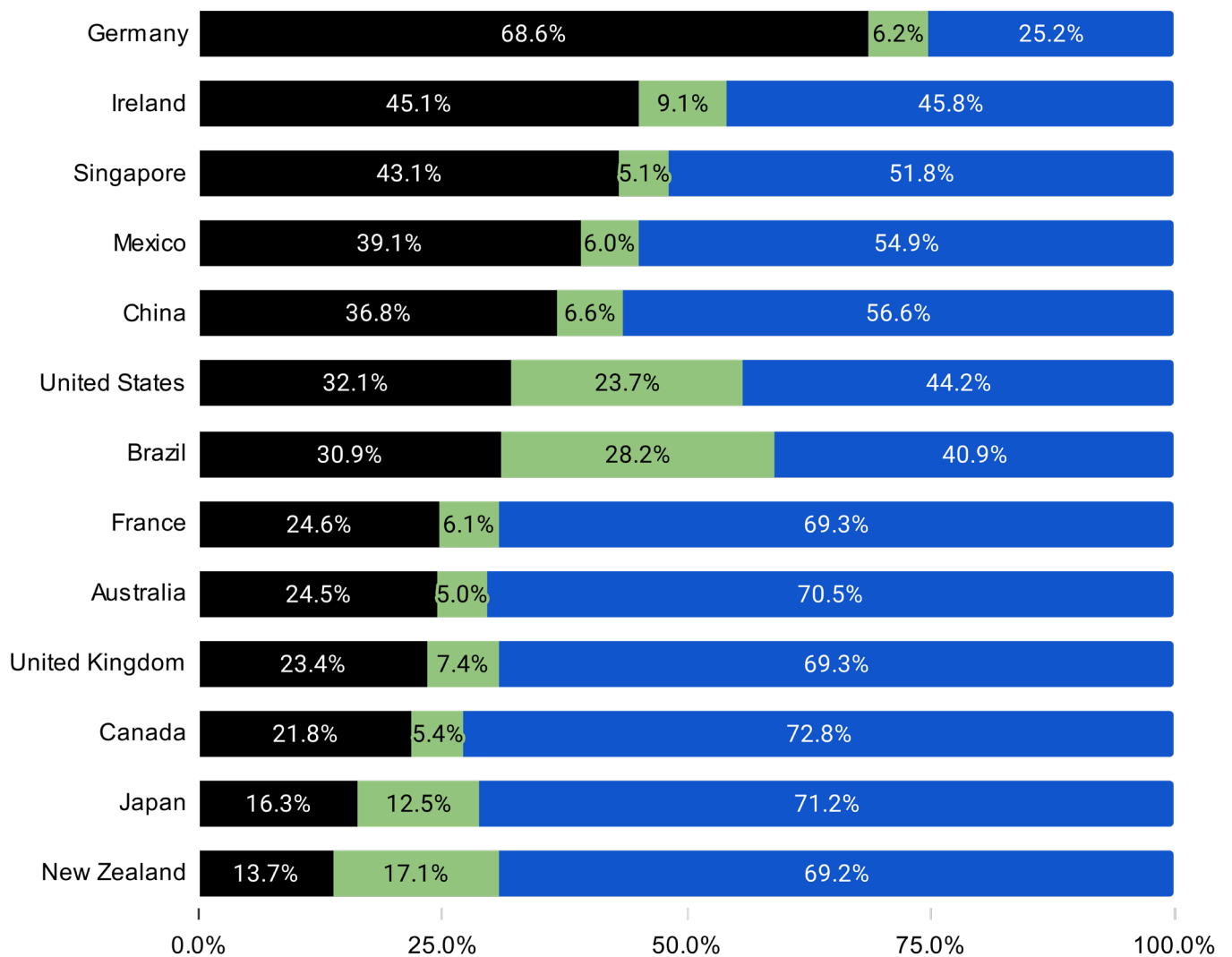
# The bad bot landscape

## Bad bots across the globe

Let us take a look at the distribution of traffic at the national level. We have sampled 13 countries and learned that 7 of the 13 have had bad bot traffic levels exceeding the global average of 30.2%. Astoundingly, Germany and Ireland had over 60% of traffic originating from bad bots. The United States too saw a slightly higher bad bot traffic ratio than the global average of 32.1%.

### Bad Bot v Good Bot v Human Traffic 2022 – by Target Country

● Bad bot ● Good bot ● Human

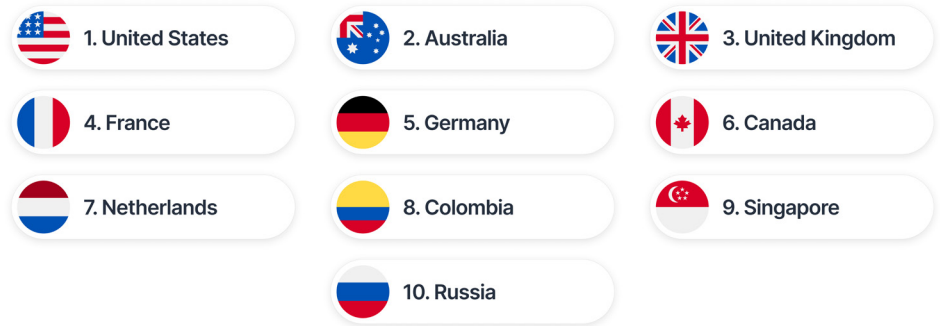


# The bad bot landscape

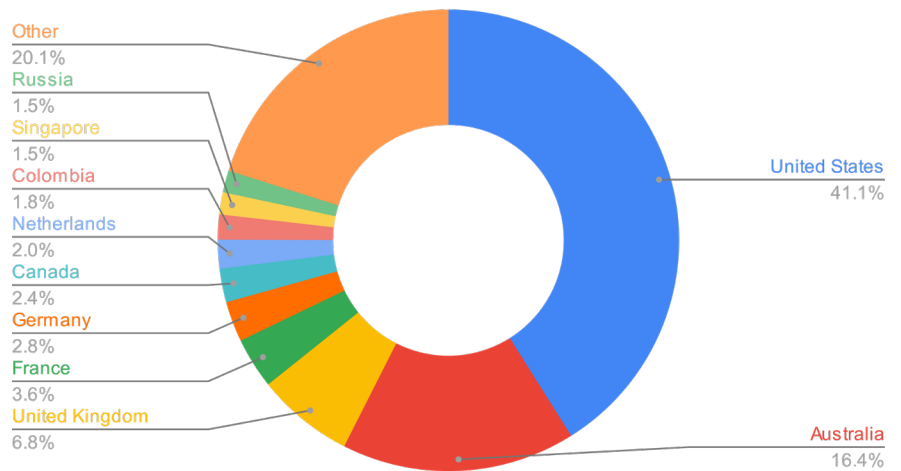
## The United States and Australia were the most targeted countries

The United States remains a top-priority target of bot attacks, as 41.1% of attacks were directed at US-based websites. That is only slightly lower than in 2021, in which 43.1% of bot attacks targeted US-based websites. Australia was the second most attacked country by bad bots again this year, targeted by 16.4% of bot attacks. That is a significant increase over last year's 6.8%. The United Kingdom was the third most targeted country, with 6.8% of attacks targeting it, very similar to last year (6.7%).

### Top 10 Most Attacked Countries by Bad Bots



### Most Bot Attacks By Target Country (2022)

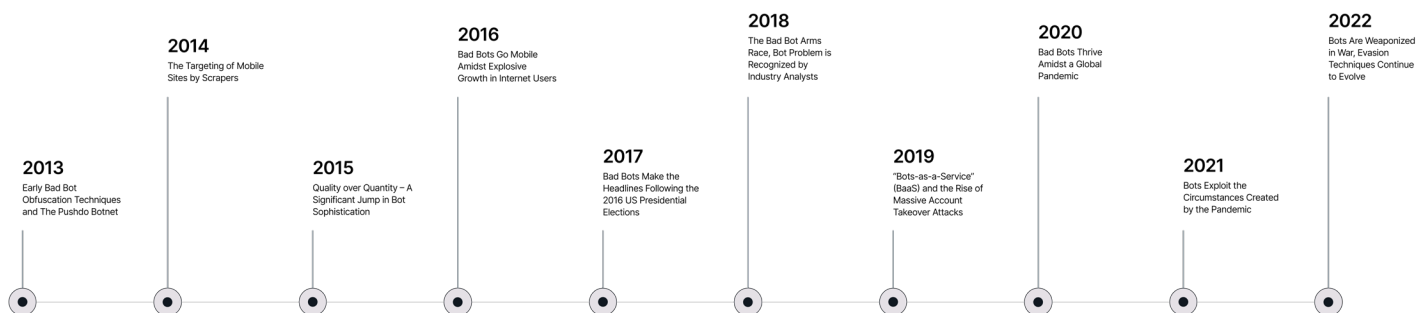




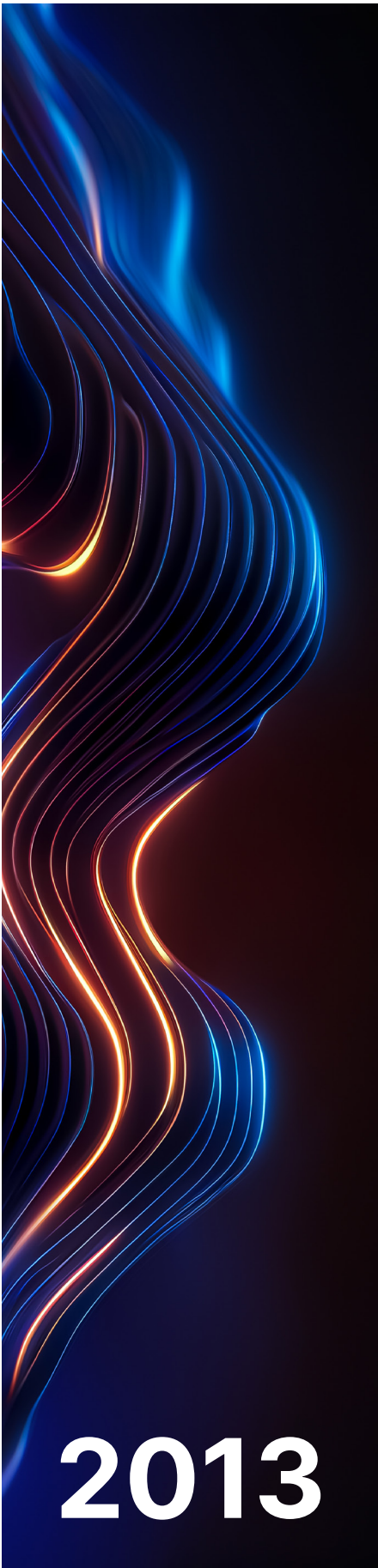
## A 10-Year Evolution of Malicious Automation

Bad bots have come a long way since the EarthLink Spammer was discovered back in 2000. That botnet, created by a single individual, sent over a million emails in a phishing scam meant to lure people into providing sensitive personal information. These bots have since then evolved into sophisticated and complex programs, often run by multinational criminal enterprises that make millions of dollars while posing severe risks to the bottom line, security, and availability of businesses across all sectors.

In this section, we will cover the evolution of bad bots over the past decade, as recorded by Imperva and Distil (acquired by Imperva in 2019) – from their increasing sophistication to their ventures into new markets and use cases.







---

# Early Bad Bot Obfuscation Techniques and The Pushdo Botnet

The first-ever Bad Bot Report covered the increase in bad bot traffic levels as well as spotlighting the early evolution of bot obfuscation, mainly by masking their user agent as a legitimate web browser. Unsurprisingly, since mobile browsing was not as widely adopted as it is today, the top three browsers were all desktop-based: Firefox, Internet Explorer (Rest In Peace), and Chrome. While mobile browsing had not yet evolved, bots being launched from mobile ISPs served as a hint of things to come in the future: during this year, the mobile bad bot threat started gaining traction, as bad bots were running across 9 of the world's top 10 mobile operators.

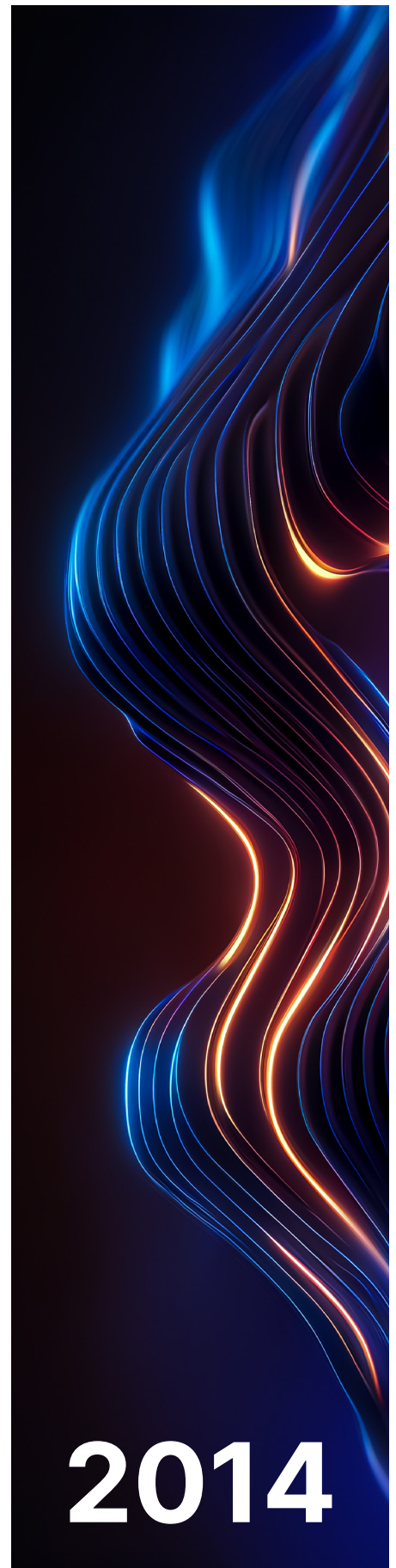
In 2013, The Pushdo bot (botnet) was the most widespread bad bot and impacted the most internet users. The Pushdo botnet infected 4.2 million IPs, which correlates to approximately 4 million actual computers being compromised. We captured Pushdo traffic coming from 15,000 different ISPs, hosting providers, and other organizations worldwide. Many companies, organizations, and government agencies were infected, including US government agencies and military networks. The purpose of Pushdo was to act as a means for sending out spam or malicious Trojans. The latter includes SpyEye and Zeus, which are notorious for lifting financial credentials from end-user computers. Serving as the underlying infrastructure for bad bots, the organization that developed and ran Pushdo stood to earn significant revenue by offering the infrastructure to the highest bidder on a revolving basis.

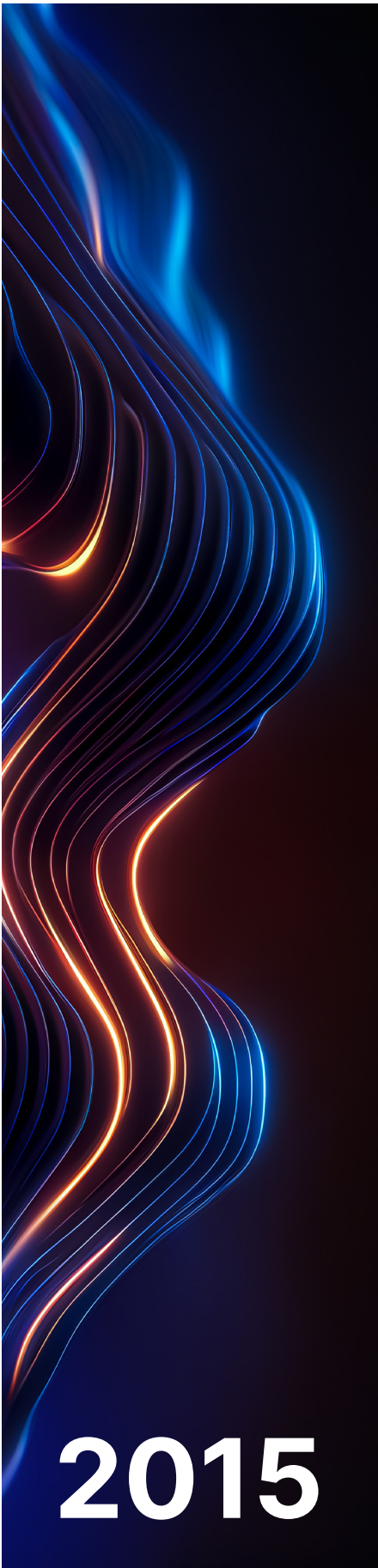
---

# The Targeting of Mobile Sites by Scrapers

We saw one of the very first examples of bots capitalizing on settings and configurations that were created to both improve and secure the browsing experience for human users. During this year, we discovered that the same characteristics that make an optimized mobile site easy to quickly navigate for humans also made them prime targets for bad bots. Mobile sites tend to be easier to scrape because they provide more structured access to website data. This was the first year that a mobile browser, the Android Webkit Browser, at 4.87%, entered into the top five list of user agents leveraged by bad bots to hide their identities.

During this year, we began tracking and analyzing bad bot traffic by their level of sophistication, classifying them as either simple, average, or sophisticated. “Simple” bad bots show their hand in several ways, such as leveraging bad user agents or failing basic browser integrity checks. “Average” bad bots can be stopped by forcing them to prove they are using a real web browser, while “sophisticated” bad bots closely mimic human behavior.





---

# Quality over Quantity – A Significant Jump in Bot Sophistication

Bot sophistication levels took a significant leap forward in 2015. They became much more sophisticated than in the past. This year marked a noticeable shift in bot technology, with roughly 11% of bad bots making the jump from simple to the next level of sophistication. We concluded that bot operators focused on bot quality, as opposed to quantity. For example, a single sophisticated bot might cycle through 1,000 IP addresses to make one request per address, instead of using a single IP address to make 1,000 requests.

We also concluded that this increasing sophistication of bots would end up skewing marketing analytics. The reason for this is the bad bot's ability to load external assets such as JavaScript. Many analytic tools, such as Google Analytics, function via a JavaScript code snippet. If bots could load these resources, we predicted that they would end up skewing analytic tools and throwing off key business and operational metrics. Based on this 2015 data, 53% of bad bots were falsely attributed as humans in Google Analytics and similar tools. As time passed, this prediction came true and has become one of the most prevalent negative effects of unmanaged bot traffic today.

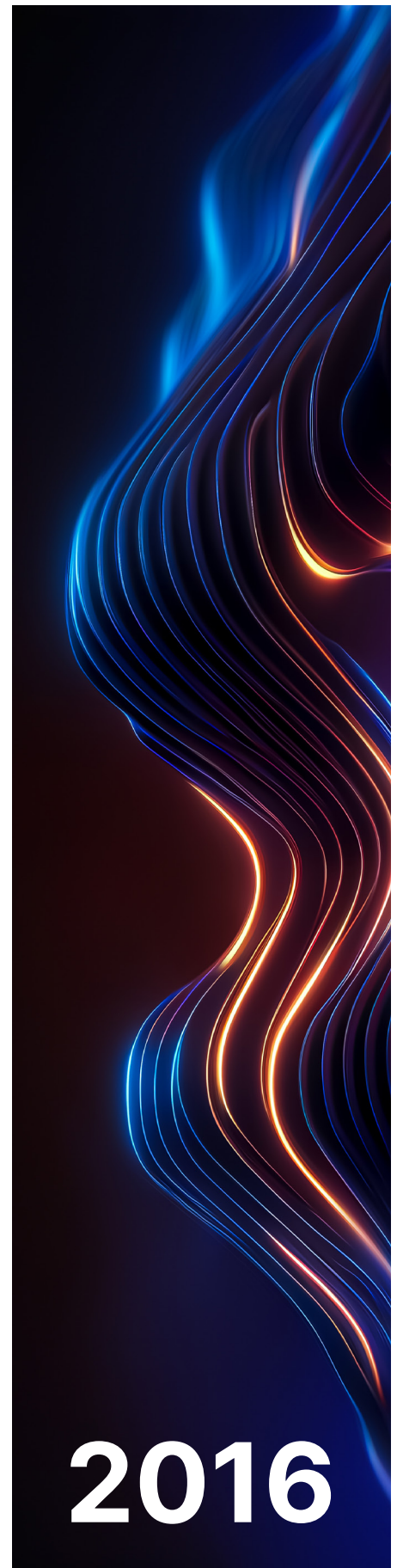


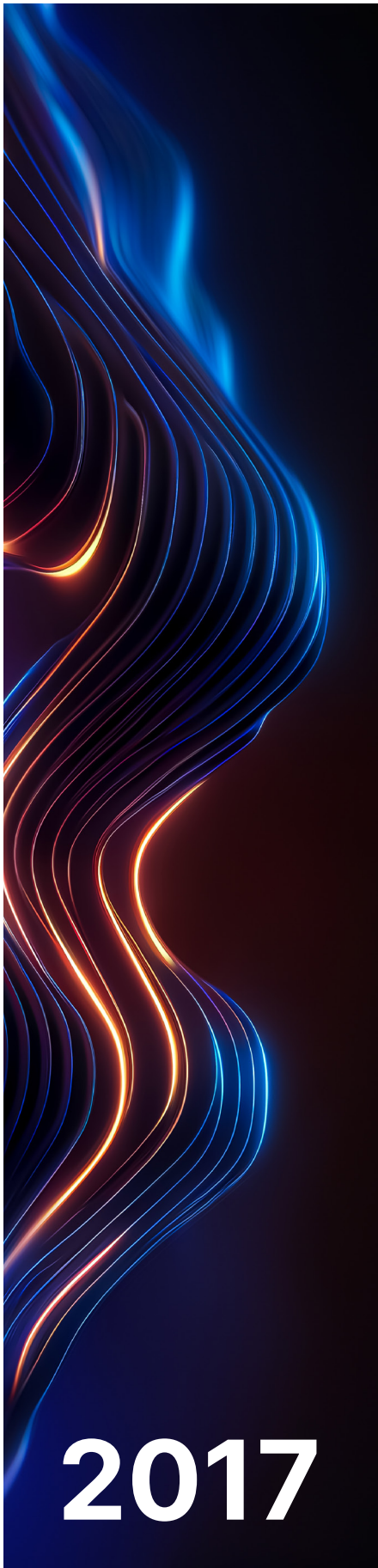
---

# Bad Bots Go Mobile Amidst Explosive Growth in Internet Users

While the percentage of bad bot traffic increased in 2016, its proportion relative to other traffic remained relatively constant. The reason for that is more people were coming online from developing nations. In 2016, approximately 185 million new internet users came online. All were using multiple devices (including smartphones, tablets, work and personal laptops) to access the internet.

Mobile web browsing overtook desktops for the first time in 2016, and bad bots soon followed suit. We saw a 42.78% year-over-year increase in bad bots claiming to be mobile browsers, as 16.1% of bad bots self-reported as mobile users – a trend we predicted would persist. Mobile ISPs accounted for 9.4% of bad bot traffic. For the first time, mobile Safari made the top five list of self-reported user agents, outranking web Safari by 17%, and claiming the third spot in the list of most popular browsers used by bad bots.





---

# Bad Bots Make the Headlines Following the 2016 US Presidential Elections

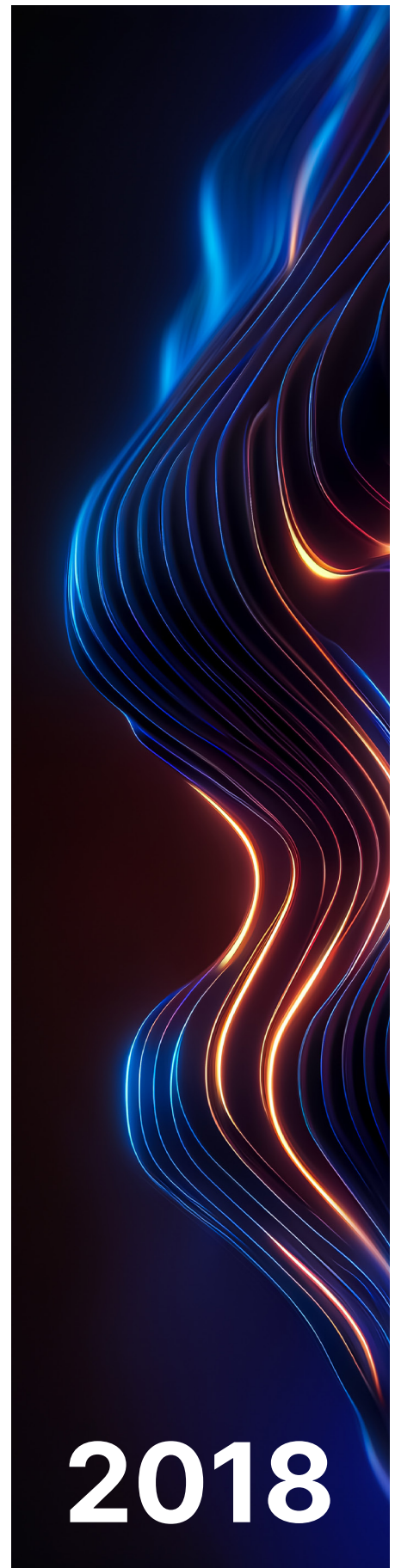
Bots made headlines following the 2016 US presidential elections. It would have been difficult for anyone to claim ignorance of the term 'bots', as they were no longer solely the concern of cyber security experts. During that year, even the FBI was investigating the use of bots to influence the results of the 2016 US presidential election. A few of the most popular social media brands were even hauled before the US Congress because bots that exploited their platforms were used to amplify and spread fake news. But while the political world attempted to understand the impact of bad bots on democracy, much of their wider impact on the economy was still misunderstood and underestimated.

---

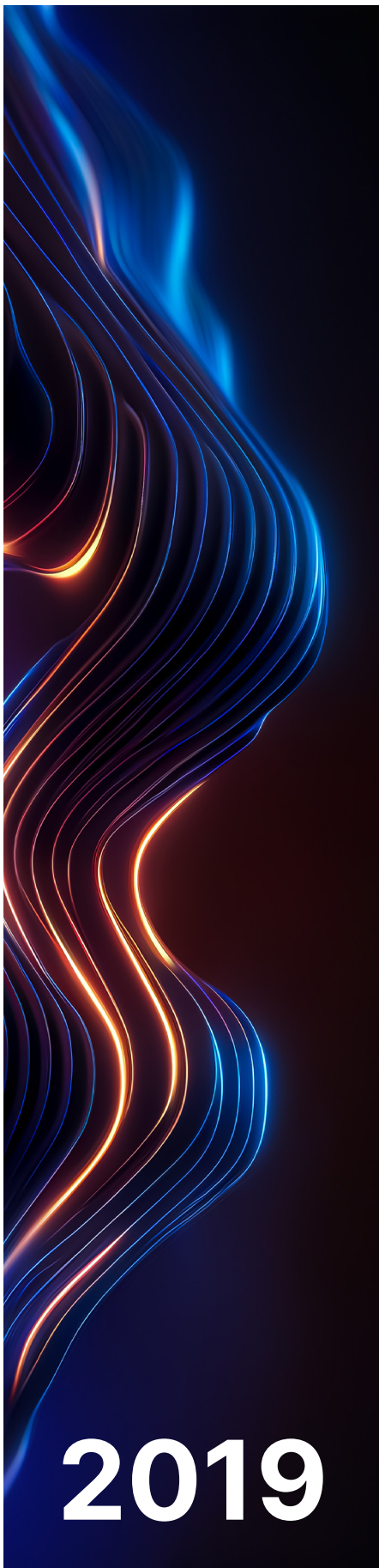
# The Bad Bot Arms Race, Bot Problem is Recognized by Industry Analysts

Bad bots became much more self-aware. It wasn't just about appearing as a legitimate user anymore; now bots had an extra layer of mimicking real human workflows across web applications to "behave" like real users. They were also able to obfuscate their activity by reverse-engineering detection systems. Advanced bots showed definitive behavior that they knew about the technology they were trying to defeat, and they continuously learned how to adapt their tactics. For example, there were more occurrences of globally distributed botnet attacks, using tactics like single request attacks, user agent rotation, random mouse movements, and page scrolling, to name a few.

This was the year that marked the end of the days of only needing to consider DDoS and web application firewall (WAF) solutions. During this year, the major industry analyst firms acknowledged that bot management was a blind spot in the cybersecurity landscape. They began recommending that addressing bad bots is a key component for comprehensive web application security. Then in Q3 2018, Forrester released its first evaluation of bot management vendors.







---

# “Bots-as-a-Service” (BaaS) and the Rise of Massive Account Takeover Attacks

Some bad bot operators, specifically in the scraping sector, attempted to rebrand bad bots in an effort to legitimize their activity as a valid business practice. This rebranding of “bots-as-a-service” manifested itself in several ways. First, through the adoption of professional-looking websites offering business intelligence services called pricing intelligence, alternative data for finance, or competitive insights. Typically, these businesses offered data products focused on specific industries. Second, there was increased pressure to purchase scraped data within your industry. No business wants to lose market share because the competition has access to data that is available for purchase. Finally, there was the growth of job postings looking for people to fill positions with titles like Web Data Extraction Specialist or Data Scraping Specialist.

Beyond content and price scraping, the biggest bad bot problem during that year was account takeover attacks. Every website with a login page is subject to these attacks, as a new phenomenon emerged during the year – the rise of mega credential stuffing attacks. One such attack, mitigated by Imperva during that year, lasted 60 hours and included 44 million login attempts. In general, the availability of billions of breached credentials has helped fuel the rise in credential stuffing, but such large-scale attacks can cause significant infrastructure strain leading to slowdowns or downtime. These large application layer credential stuffing attacks are as damaging as volumetric DDoS attacks to any organization that is unprepared to handle such a high volume of bad bot requests.



---

# Bad Bots Thrive Amidst a Global Pandemic

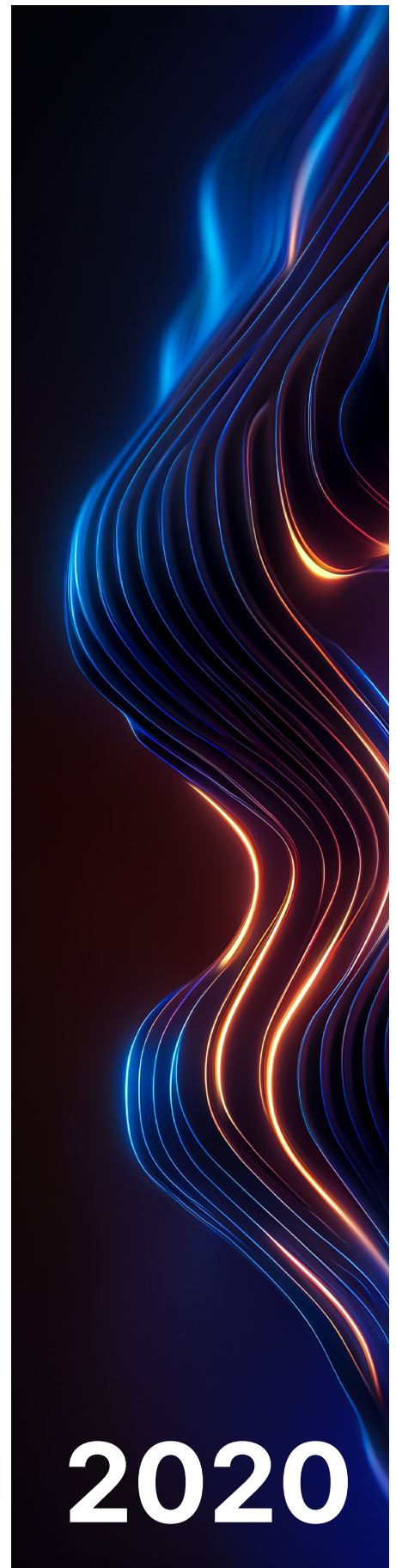
The global pandemic set the stage for an evolution in how bad bots were being used, as bot operators were forced to find new income sources. While some of their most precious targets had been shut down, like travel and ticketing, bot operators had new opportunities to target new segments and exploit the panic caused by the pandemic. From fake news spam campaigns to scalping of commodities and targeting vaccine appointments – bots were busier than ever.

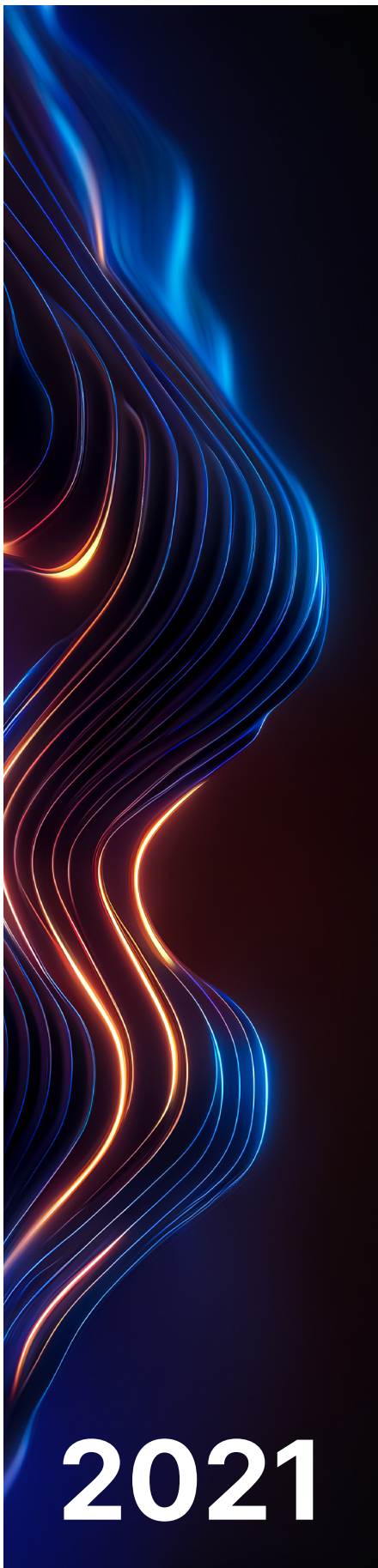
In the very early days of the pandemic, we identified bad bots posting comment spam on social media, leading to concerns over a global spread of fake pharmacy fraud. Social media bots were also used to spread fake news ranging from the connection between 5G and Coronavirus to stories of hospitals being filled with mannequins. Oftentimes, these messages included links that led to phishing attacks. The World Health Organization (WHO) has dubbed the spreading of misinformation an “infodemic.”

We also noticed that scalpers deployed bots to hoard large inventories of face masks, sanitizers, detergents, home workout equipment, and more. N95 masks specifically were targeted after being recommended by WHO and were impossible to find in-store or online at MSRP.

As vaccines began rolling out, we monitored a 372% increase in bad bot traffic on healthcare websites globally. In particular, we observed indications of bot activity on websites that offer vaccine appointment availability. This sparked a worldwide discussion about the thin line between good bots and bad ones. Individuals and companies created bots to find available vaccine appointments. These helpful bots were created with good intentions, but it isn't far-fetched to imagine others creating similar tools or using existing ones to sell appointments to the highest bidder.

Towards the end of 2020, we saw bots take advantage of the global chip shortage, which lasted well into 2022. This increased the popularity of scalping bots even further during the pandemic, creating the perfect storm for them to thrive. As the supply of semiconductor chips failed to meet demand, it affected over 169 industries, leading to major shortages and queues among consumers for graphics cards, video game consoles, cars, and other electrical devices. This, combined with other factors, made bad bots aggressively target the gaming hardware market in the second half of 2020 and throughout the holiday season, with a peak in attacks clearly seen in October 2020. This made it the month with the highest number of bad bot incidents on online retail websites that year. For frustrated consumers, getting a new gaming console or a GPU for the holiday season was an almost impossible task made even harder by the increase in bad bot attacks.





---

# Bots Exploit the Circumstances Created by the Pandemic

The pandemic created a fertile ground, ripe with new opportunities for bot operators. As a result, we saw bots expanding to new markets and use cases. One such market is government services. These services suffered during the pandemic, leading to a backlog that continues to this day, making the process of scheduling an appointment an absolute nightmare for those in need of these services. Passports, in particular, have been a worldwide issue. As many passports across the world expired during the pandemic, this created a surge of people in need of new passports once travel restrictions were lifted. Other examples of this backlog were seen in visa appointments across Europe and driving tests in the UK, among others. 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.

Imperva recorded and mitigated 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 15-20 times 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. Cybercriminals then attempted to sell these appointment slots for upwards of €400. The consequences of not being able to schedule such appointments are severe, preventing legitimate individuals from securing their visas, and risking them living in the country illegally.

In another case, bots were used for a large-scale fraudulent operation, in an attempt to take advantage of the COVID relief funds provided to students of higher education by the US Congress. Significant portions of these federal emergency grants were provided to students to help with food, housing, course materials, technology, healthcare, and childcare. These funds were meant to serve students and ensure learning continued during the COVID-19 pandemic. 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. This type of online fraud is referred to by the OWASP as OAT-019 Account Creation. This is yet another example of how bot operations have evolved during the pandemic and in its aftermath.

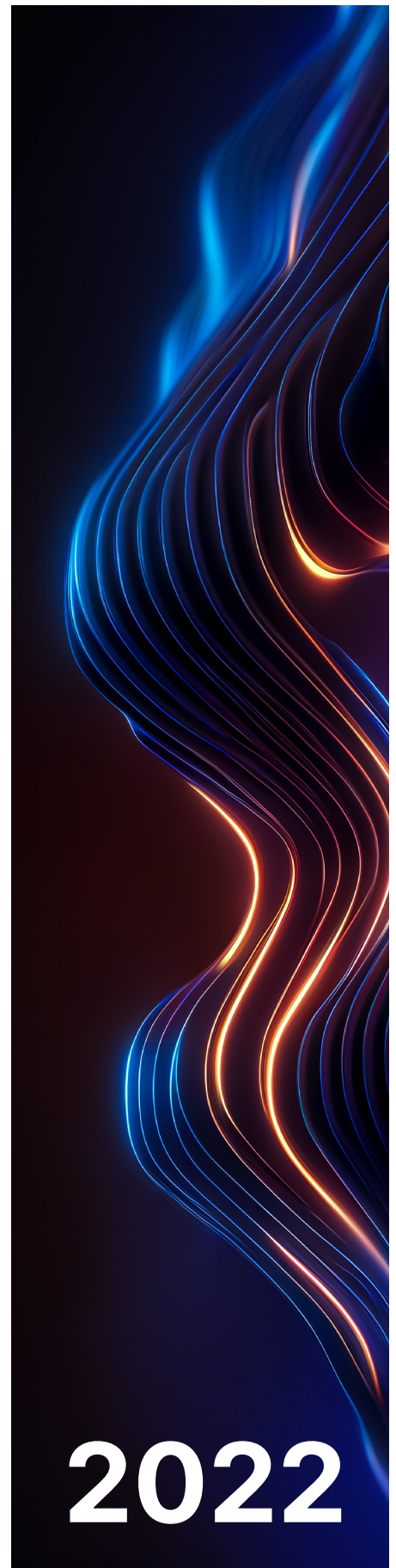
---

# Bots Are Weaponized in War, Evasion Techniques Continue to Evolve

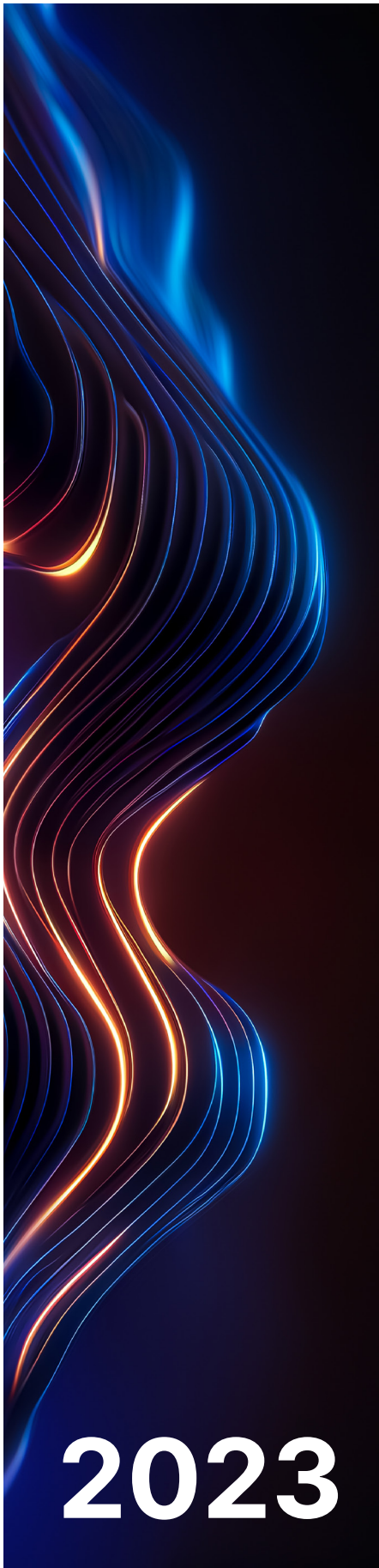
In early 2022, as the war in Ukraine began, the Imperva threat research team observed a 145% spike in automated attacks targeting Ukrainian web applications. These attacks were likely intended to disrupt services. The recorded attacks made use of advanced bots that facilitate distributed denial of service (DDoS) attacks, fraud, and malicious code injections. These attacks are usually aimed at denying critical services across the financial, telecom, and energy sectors. Additionally, Imperva recorded and stopped two massive Account Takeover attacks meant to compromise Ukrainian users' accounts.

During this year, we have also noticed a significant increase in the number of bad bots choosing Mobile Safari as their preferred disguise. The reason for this is the additional privacy settings provided by this browser, which sends fewer attributes to the origin. During the early reconnaissance phase of an attack, bot operators simulate each step of a human user's request. The simulation enables them to observe the major differences between each browser. This leads them to surmise that there are fewer attributes sent from the iOS request compared to other web clients, resulting in the implementation of that rotation in their scripts. Some browser automation tools, like Puppeteer, for example, go a long way toward supporting these attacks by adding script browser overrides that further assist attackers in mimicking iOS as much as possible.

Still, that alone isn't sufficient. Now more than ever, we are seeing bad bots employ a wide variety of evasion methods, including frequently cycling through IP addresses, hiding behind anonymous proxies and peer-to-peer networks, and manipulating their login parameters and cookies to make it appear as if the requests are being made from different browsers, changing their user agents, and more. Today's most sophisticated bad bots can even evade or solve CAPTCHA challenges through integrations with various tools and platforms.







---

# Bad Bots Are Coming For APIs

We predict that APIs will become the prime target for bad bots in 2023. In pursuit of sensitive data, cybercriminals will put more focus on vulnerable API endpoints that connect directly to an organization's underlying database. Because API security defenses often overlook automated threats, bots will become a persistent challenge next year and generate more scrapping attacks on individual APIs that lead to data leakage. The challenge is that returning a CAPTCHA challenge to an API request breaks the calling application. Thus, machine learning will be needed to differentiate normal API behavior from malicious traffic, and to understand what data should be transmitted through the API. Therefore, organizations will be challenged to mitigate automated attacks targeting their API libraries until bot management and API security are used in concert.

To summarize, it is clear that bad bots' sophistication has come a long way, significantly evolving over the course of the past 10 years. But their increasing sophistication isn't the only way in which they have evolved. What started as botnets that are used for massive email phishing campaigns have evolved to encompass over [20 use cases](#), targeting every industry and affecting multiple stakeholders, not just security.

# 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. However, there are some proactive steps you can take to start addressing the problem today.

## 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 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, announcing a date and time for a coveted product launch will attract bots trying to get their hands on it first. Make sure that you are prepared to handle the high volume of traffic, including a high ratio of evasive bots trying to scoop up the products and deny your customers access.
- **B** – 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. Ensure 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 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:

|                           | <b>BLOCK</b><br>End of Life more than 3 years | <b>CAPTCHA</b><br>End of Life more than 2 years |
|---------------------------|---|---|
| Chrome version            | <85   | <95   |
| Firefox version           | <78   | <91   |
| 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, LLC.

## 5. Threat Reduction: Automation

Automation tools such as Selenium, Web Driver and others are clear signs of bot traffic.

## 6. Evaluate Traffic

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

## 7. Monitor Traffic

- **A** – 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.
- **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

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.

## 9. Evaluate Bot Mitigation Solutions

In the early days of bot attacks, 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.

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.

# Appendix

## Bad bot use cases

| Bad bot problems        | What is it  | How it hurts the business   | Symptoms   | Targeted industries  |
|-------------------------|---|---|--|--|
| <b>Price Scraping</b>   | The use of bots to illegally monitor and track pricing information, typically in order to undercut rivals and boost sales | <p>Loss of sales to competitors that scrape your prices, undercut them and beat you in the marketplace</p> <p>Damaged reputation due to scraped data being used in a way that misrepresents the business's prices or products</p> <p>The lifetime value of customers worsens</p> <p>Impacts website performance</p> | <p>Declining conversion rates</p> <p>Your SEO rankings drop</p> <p>Unexplained website slowdowns and downtime (usually caused by aggressive scrapers)</p>          | <p>All businesses that show pricing:</p> <ul style="list-style-type: none"><li>• Retail</li><li>• Gaming</li><li>• Airlines</li><li>• Travel</li></ul>   |
| <b>Content Scraping</b> | The use of bots to extract content and data from a website  | <p>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</p> <p>Duplicate content damages your SEO rankings</p> <p>Damage to brand reputation</p> <p>Impacts website performance</p>         | <p>Your content appears on other sites</p> <p>Your SEO rankings drop</p> <p>Unexplained website slowdowns and downtime (usually caused by aggressive scrapers)</p> | <p>Similar to Price Scraping, but in addition:</p> <ul style="list-style-type: none"><li>• Job boards</li><li>• Classifieds</li><li>• Marketplaces</li><li>• Finance</li><li>• Ticketing</li></ul> |



|  |   |   |  |   |
|--|---|---|--|---|
| <b>Account Takeover (aka Credential Stuffing, Credential Cracking)</b> | 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  | Increase in failed login rates   | Any business with a login page  |
|  |   | Customer frustration to due account lockout, data theft or dealing with fraudulent, increasing churn                                    | Increase in customer account lockouts and customer service tickets                   |   |
|  |   | Impacts website performance, availability and reliability   | Increase in fraud (lost loyalty points, stolen credit cards, unauthorized purchases) |   |
|  |   | Risk of noncompliance with data privacy regulations   | Increase in chargebacks  |   |
|  |   | Increased support and fraud costs   |  |   |
| <b>Account Creation (aka Account Aggregation, New Account Fraud)</b>   | 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            | Abnormal increases in new account creation   | Messaging platforms <ul style="list-style-type: none"> <li>• Social media</li> <li>• Dating sites</li> <li>• Communities</li> </ul> |
|  |   | Loss of revenue to bots that exploit new account promotion credits (money, points, free plays)  | Increased comment spam   | Sign-up promotion abuse <ul style="list-style-type: none"> <li>• Gaming</li> <li>• Finance</li> </ul>                               |
|  |   | Metrics based on the number of user accounts or social media interactions that all originate from bots may lead to poor decision making | Drop-in conversion rates from new accounts to paying customers                       |   |

|   |  |  |  |   |
|---|--|--|--|---|
| <b>Credit card fraud (aka Carding, Card Cracking)</b> | 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      | Rise in credit card fraud<br>Increase in customer support calls<br>Increased chargebacks processed   | Any site with a payment processor:<br><ul style="list-style-type: none"> <li>• Retail</li> <li>• Nonprofit/Charities</li> <li>• Airlines</li> <li>• Travel</li> <li>• Ticketing</li> <li>• Finance</li> <li>• Gaming</li> </ul> |
|   |  | 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.)  |  |   |
| <b>Denial of Service</b>                              | 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<br>Lost revenue from the unavailability of websites<br>Damaged brand reputation  | Abnormal and unexplained spikes in traffic on particular resources (login, signup, product pages, etc.)<br>Increase in customer service complaints | All industries  |
|   |  | Potential customer churn   |  |   |
| <b>Gift Card Balance Checking and Abuse</b>           | The use of bots to automate the enumeration of potential gift card numbers against balance checking pages to steal gift card balances  | Similar to credit card fraud, gift card fraud leads to financial losses due to bots that steal money from gift cards<br>Increased customer service costs to process fraudulent chargebacks | Spike in requests to the gift card balance page<br>Increase in customer service calls about lost balances  | Any business offering gift cards as a payment option - Retail predominantly   |
|   |  | Poor customer reputation and loss of future sales  |  |   |
|   |  | Damaged brand reputation   |  |   |

|                            |  |  |   |   |
|----------------------------|--|--|---|---|
| <b>Denial of Inventory</b> | 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  | Increase in abandoned items held in shopping carts                                      | Businesses offering scarce or time-sensitive items:   |
|                            |  | Lower conversion rates   | Decrease in conversion rates  | <ul style="list-style-type: none"> <li>• Airlines</li> <li>• Tickets</li> <li>• Retail</li> <li>• Healthcare</li> </ul>   |
|                            |  | Increased cart abandonment rates   | Increase in customer complaints about lack of availability of inventory                 |   |
|                            |  | Damaged customer reputation because unscrupulous middlemen hold all inventory until resold elsewhere   |   |   |
| <b>Scalping</b>            | The use of bots to gain an unfair advantage over legitimate consumers and obtain limited-availability and/or preferred goods/services      | Damaged customer reputation  | Unexplained website slowdowns and downtime (usually caused by aggressive scalping bots) | Similar to Denial of Inventory:   |
|                            |  | Slows the website performance causing brownouts or downtime, leading to loss of revenue  | Decrease in conversion rates  | <ul style="list-style-type: none"> <li>• Airlines</li> <li>• Tickets</li> <li>• Retail</li> </ul> E.g. sneakers, consoles, computer hardware, limited edition items. <ul style="list-style-type: none"> <li>• Healthcare</li> </ul> |
|                            |  | Lower lifetime value (LTV), because a bot doesn't regularly come back for additional items   | Increase in customer complaints about lack of availability of inventory                 |   |
|                            |  | Lower average basket value (ABV), because bots target a single product as opposed to legitimate consumers that tend to purchase additional items |   |   |

## Bad bot by industry

| Bad bot problems            | What is it  | How it hurts the business   |
|-----------------------------|---|---|
| <b>Automotive</b>           | Manufacturers, dealerships, vehicle marketplaces                                      | Price scraping, data scraping, inventory checking   |
| <b>Business Services</b>    | Real estate, third party vendors like retail platforms, CRM systems, business metrics | Attacks targeting APIs, data Scraping, account takeover   |
| <b>Computing &amp; IT</b>   | IT services, IT providers, services and technology providers                          | Account takeover, scraping  |
| <b>Education</b>            | Online learning platforms, schools, colleges, universities                            | Account takeover for students and faculty, class availability, scraping proprietary research papers and data                    |
| <b>Entertainment</b>        | Streaming services, ticketing platforms, production companies, venues                 | Account takeover, price scraping, inventory scraping, scalping  |
| <b>Financial Services</b>   | Banking, insurance, investments, cryptocurrency                                       | Account takeover, carding, card cracking, custom content scraping   |
| <b>Food &amp; Groceries</b> | Food delivery services, online grocery shopping, food & beverage brand sites          | Credit card fraud, gift card fraud, account takeover, coupon guessing   |
| <b>Gambling</b>             | Casinos, sports betting   | Account takeover, odds scraping, account creation for promotion abuse,  |
| <b>Gaming</b>               | Online gaming, video games  | Account takeover, account creation for promotion abuse and cheating, gaming automation, denial-of-service                       |
| <b>Government</b>           | Law & government websites, citizen services, states, municipalities, metropolitans    | Account takeover, data scraping of business registrations listings, voter registration, appointment scraping and scheduling     |
| <b>Healthcare</b>           | Health services, pharmacies   | Account Takeover, Content Scraping, "Helpful" bots that scrape for appointment availability                                     |
| <b>Lifestyle</b>            | Lifestyle magazines, blogs  | Proprietary content scraping  |
| <b>Marketing</b>            | Marketing agencies, advertising agencies  | Proprietary content scraping, ad fraud, denial of service, skewing  |
| <b>News</b>                 | News sites, online magazines  | Proprietary content scraping, ad fraud, comment spam  |
| <b>Retail</b>               | eCommerce, marketplaces, classifieds  | Account takeover, scalping, denial of inventory, credit card fraud, gift card fraud, data and price scraping, analytics skewing |

|                                |  |  |
|--------------------------------|--|--|
| <b>Community &amp; Society</b> | 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 |
| <b>Sports</b>                  | Sports updates, news, live score services  | Data scraping (live scores, odds etc.)   |
| <b>Telecom &amp; ISPs</b>      | Telecommunications providers, mobile ISPs, hosting providers                                   | Account takeover, competitive price scraping   |
| <b>Travel</b>                  | Airlines, hotels, holiday booking  | Price and data Scraping, skewing of look-to-book ratio, denial of service, price scraping, account takeover  |

# Imperva Threat research

## Imperva Global DDoS Threat Landscape

### Key Findings

Application layer DDoS attacks increased by 82% compared to 2021.



## The State of Security within eCommerce

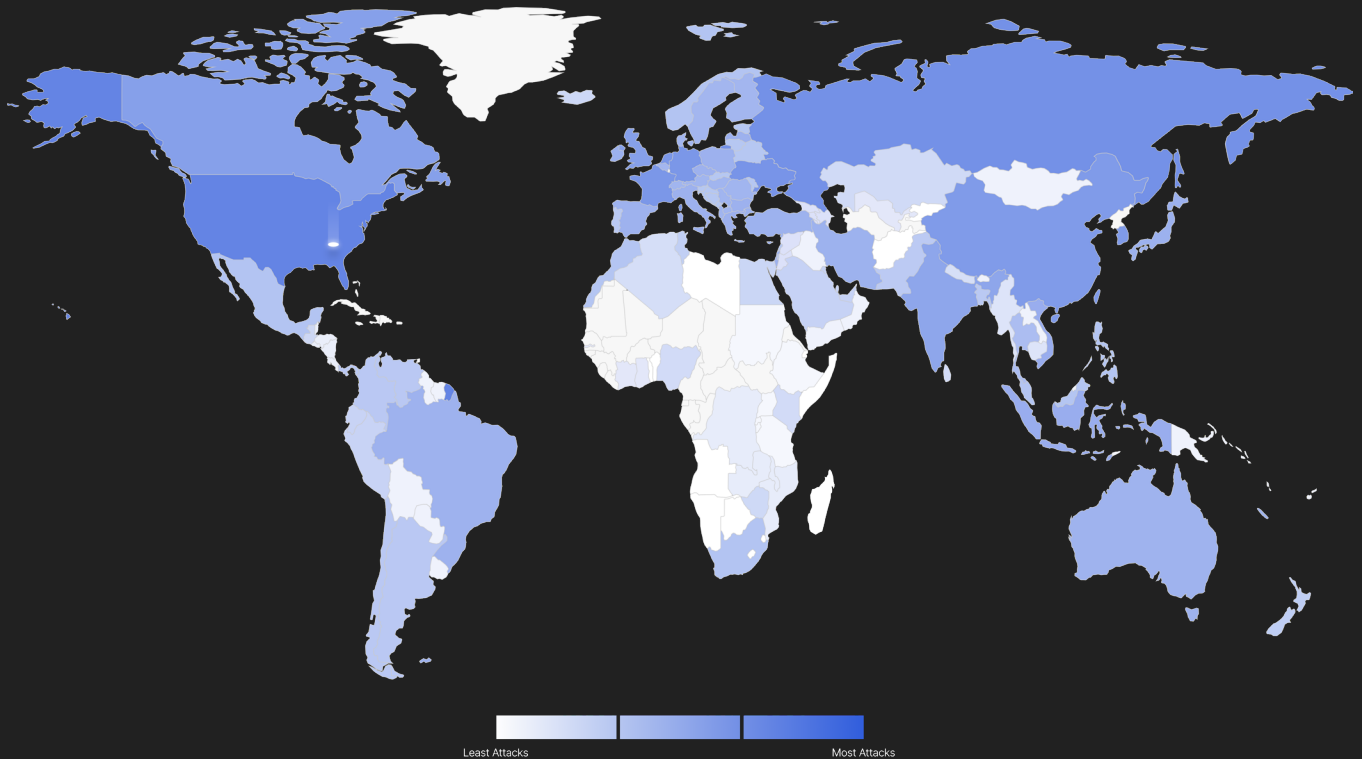
### Key Findings

62% of attacks on online retailers were automated attacks



## 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 cybersecurity leader that helps organizations protect critical applications, APIs, and data, anywhere, at scale, and with the highest ROI. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey. Imperva Threat Research and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate 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 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**.

© 2023 Imperva, Inc. All rights reserved.  
Imperva is a registered trademark of Imperva, Inc.