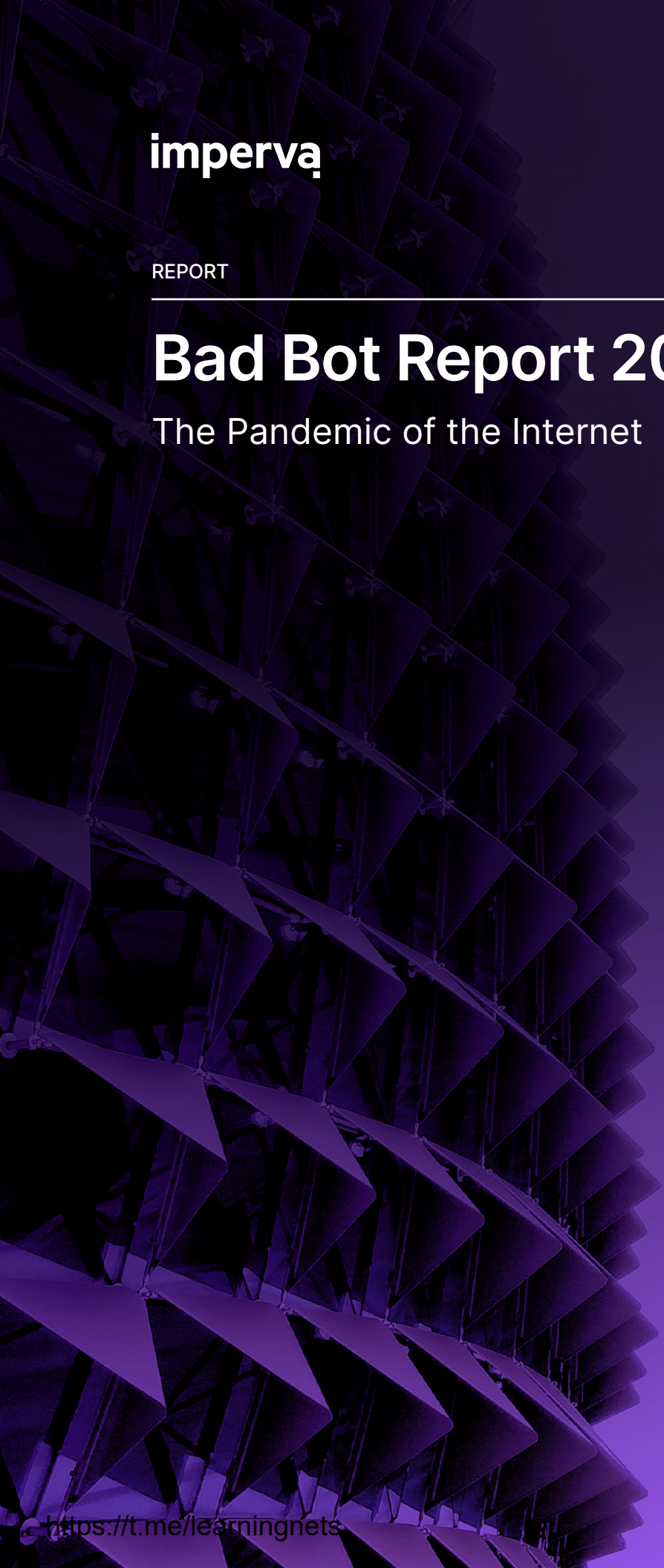


imperva

REPORT

Bad Bot Report 2021

The Pandemic of the Internet

Contents

ABOUT THE BAD BOT REPORT 2021

Imperva's Bad Bot Report 2021 investigates the daily attacks that sneak past sensors and wreak havoc on websites.

This is the 8th annual Bad Bot Report. It's based on 2020 data collected from Imperva's global network, and includes hundreds of billions of bad bot requests anonymized over thousands of domains. The goal of this report is to provide meaningful and guiding information about the nature and impact of these automated threats to those of you who are in the frontlines of website security.

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

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

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

What's new in this report

This year's report is the first one published since the full integration of Advanced Bot Protection (formerly Distil) into Imperva's Application Security Platform. This integration not only enables better performance, but also provides us with a vastly larger data set. This means that data in this report is different from the data presented in previous editions in the following ways:

- **Larger volume of data:** Significantly more traffic flowed through the system in 2020 than in previous years. The outcome is that the law of large numbers causes slight changes in the statistics. This created challenges for making comparisons to previous years' data.
- **Higher volume of simple threats:** As an integrated platform that includes two layers of bot protection -- basic bot protection through Imperva's Cloud WAF and Advanced Bot Protection -- simple bots are already blocked by Cloud WAF, while Advanced Bot Protection handles the moderate and sophisticated threats. Compared to prior years, this makes for a larger portion of simple bots when dissected by sophistication levels.
- **New highlight detection feature:** The tool developed by the Threat Research Labs allows us to track noteworthy events and provide important insights.

Scalpers exploit the pandemic

Bad bots are the major pandemic ravaging the internet. Their notorious ability to mimic human interactions in highly persuasive ways helps them remain undetected. These automated threats consistently top the list of concerns for many businesses and security practitioners. Bad bots have been thriving throughout the global pandemic, targeting new markets and hiding within the global surge in internet traffic.

In fact, together with more human internet traffic, we also saw our Advanced Bot Protection solution manage more bot traffic than ever before. For bot operators, the pandemic saw an increasing volume of business transactions online and helped identify more opportunities to use bots to make money. Specifically, scalpers took advantage of the situation—from leveraging the panic to stockpile commodities, to taking the gaming hardware market hostage due to supply shortages.

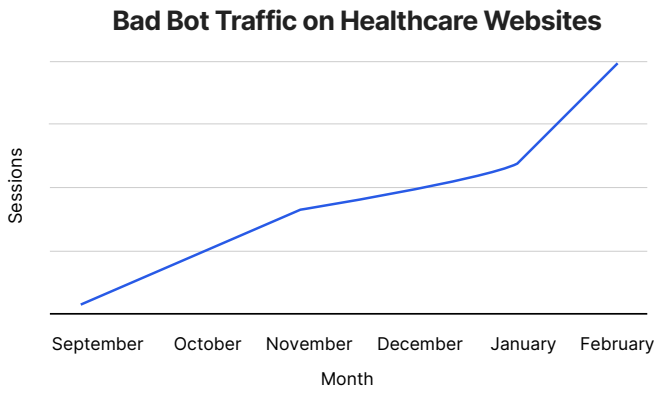
Scalping is the act of buying a high demand or limited edition product, in order to resell at a higher cost to make a profit. Bad bots are used to check for inventory and hoard any available inventory. The phenomenon that once focused on concert and sporting events tickets, and limited edition items like sneakers, has expanded to new markets.

There are two main reasons for this expansion. First, the pandemic resulted in a reduction of traditional scalpers' sources of income. Concerts and sporting events were canceled or took place without live audiences. The second reason is high demand for many products during the pandemic that weren't fulfilled by retailers due to various slowdowns along the supply chain.

During the first few weeks of the pandemic, as global panic levels began rising, we noticed that scalpers were deploying bots to hoard large inventories of face masks, sanitizers, detergents, home workout equipment, and more. N95 masks specifically were targeted after being recommended by the World Health Organization (WHO) and they were impossible to find in store or online at MSRP.

Bots that schedule vaccine appointments?

Imperva's Threat Research Labs has monitored a 372 percent increase in bad bot traffic on healthcare websites globally since September 2020. Recently, as vaccines rollout to younger age groups, we are seeing indications of bot activity on websites that offer vaccine appointment availability. We have recorded activity at rates of as much as 12,000 requests per hour.



Today, as the world takes small steps towards a return to some form of normal, the latest concerns come from the rollout of vaccines. Healthcare services, pharmacies and retailers are preparing in case they are the next major target of bad bots. For those managing the vaccine rollout, the prospect of bot operators pointing inventory hoarding bots to gain an unfair advantage and jump the line to snatch appointments are cause for concern.

The rise of the helpful bot

Individuals and companies have created automated tools like TurboVax[1] for example, a bot that finds available vaccine appointments in New York City. These helpful bots were created with good intentions, but it's not far-fetched to imagine others creating similar tools in order to sell the appointment to the highest bidder for the opportunity to jump the queue. The unanswered question is whether a resale market for vaccine appointments exists and how much is each one worth?

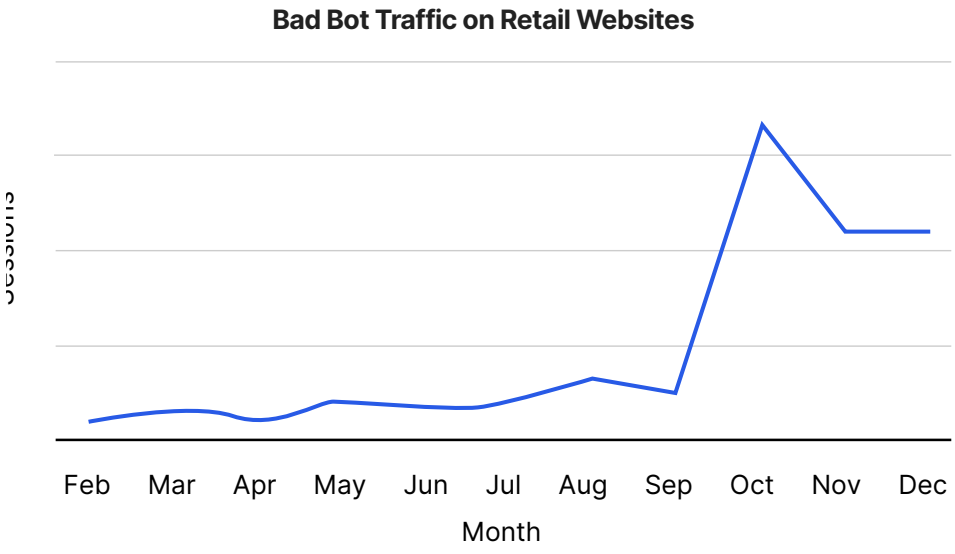
Bad bots leveraging the "infodemic" to spread fraud

At the start 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 have also been used to spread fake news ranging from the connection of 5G and Coronavirus to stories of hospitals being filled with mannequins. Often, these messages included links that led to phishing attacks. The WHO has dubbed the spreading of misinformation an "infodemic".

1 https://www.theguardian.com/us-news/2021/mar/01/turbovax-vaccine-website-huge-ma

Grinchbots make millions hoarding gaming hardware

Scalpers are now plaguing the gaming hardware market, which they targeted using Grinchbots during the holiday season. The result left many gamers frustrated because purchasing a new generation gaming console, GPU or CPU became practically impossible because bots hoarded them all. In a recent analysis of the online scalping market by data analyst Michael Driscoll, he reveals that the profits made from these sales on just a single online marketplace are estimated at US$82 million[2]. The situation is predicted to continue throughout 2021, as hardware supply remains scarce and demand grows. The chart below illustrates the grinchbot phenomenon–a gargantuan 788 percent increase in bad bot traffic to retail websites globally between September and October 2020. The timing is no coincidence, and aligns perfectly with pre-order dates for the new generation gaming consoles as well as the holiday season shopping frenzy.



The legal stance against scalpers

In the UK, Douglas Chapman MP has brought a private member's bill forward in the House of Commons to criminalise game console scalping[3]. In addition, there is an ongoing petition by Change.org, titled "Prevent/deter the buying and reselling of goods/services at inflated prices"[4]. The UK government has responded to all petitions that have garnered more than 10,000 signatures, and this one already has over 17,000. At 100,000 it will be considered for debate in the Parliament. According to an interview published on Forbes[5], scalpers are claiming injustice, stating they are only middlemen and present a legitimate business. "Nobody complains when a grocery store buys milk from a farmer and resells it for twice as much."

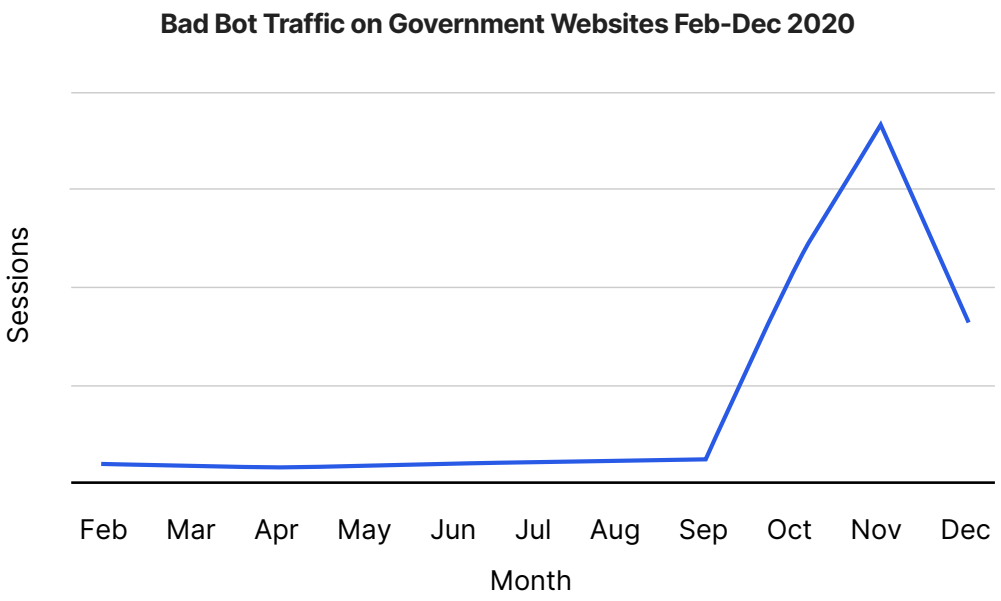
2 https://dev.to/driscoll42/an-analysis-of-the-80-million-ebay-scalping-market-for-xbox-ps5-amd-and-nvidia-f35
3 https://news.sky.com/story/shortage-of-ps5-and-xbox-consoles-drives-calls-for-scalping-to-be-criminalised-12209606
4 https://petition.parliament.uk/petitions/561986
5 https://www.forbes.com/sites/jaymcgregor/2021/02/10/playstation-5-scalpers-arent-happy-with-their-public-image/?sh=393f94012c8d

The legality of web scraping

Following the Ninth Circuit appellate court's decision in favor of allowing bots to scrape publicly available content, LinkedIn filed its petition requesting Supreme Court review in March 2020. HiQ were asked for a response by the court in April. In their opposition, HiQ stated that it is debatable whether a company can use the Computer Fraud and Abuse Act to prevent access to information that the website's users have shared on their public profiles and is available for viewing by anyone with a web browser[6]. Linkedin isn't the only social network in the fight against web scraping. In October 2020, Facebook filed a lawsuit in the U.S. against two companies engaging in an international data scraping operation. The operation's boundaries weren't limited to Facebook alone, encompassing Twitter, Amazon, LinkedIn and YouTube[7].

Bad bots targeting the elections?

Data from Imperva's Threat Research Labs reveals a significant increase in advanced bad bot traffic targeting government websites with peak traffic in November. Bad bot traffic to those websites was consistently low in volume from February to September. It is unclear what their goal was, but the timing does raise the question.



6 https://www.natlawreview.com/article/hiq-files-opposition-brief-supreme-court-linkedin-cfaa-data-scraping-dispute
7 https://techcrunch.com/2020/10/01/facebook-sues-two-companies-engaged-in-data-scraping-operations/

Account Takeover prevalence and sophistication rises

Account Takeover attacks (e.g Credential Stuffing, Credential Cracking, Dictionary) are becoming increasingly common and frequent as more PII (Personally Identifiable Information) is available online. If there is money to be made by taking over accounts on a certain website, the likelihood of an attack is high. Data from Imperva Research Labs reveals that a third of all login attempts during the last few months have been malicious. Websites face an Account Takeover attack, on average, 16 percent of the time. Nearly half (45 percent) of Account Takeover attempts originate from the U.S., with the main targets of these attacks being computing & IT services, travel, entertainment, and financial services.

Uncovering fraud through successful login investigation

It is commonly known that spikes of unsuccessful logins are bots performing Account Takeover to commit fraud. But successful logins are also valuable in uncovering fraud. Businesses must examine any user account with an abnormally high number of successful login attempts. Typical human users don't log in and out of the same account hundreds of times a day. Two behaviors are typically uncovered from examining successful login data—canary accounts and high activity accounts.

The canary account in Account Takeover attacks

The first behavior is the discovery of canary accounts created by hackers to optimize brute force attacks using Credential Stuffing and Credential Cracking techniques. These canary accounts verify whether the bot behavior has triggered any security rules on the target website. The method is simple: bot operators attempt to login using 4-5 stolen credentials, then login to their canary account. If access is denied to the canary account, it confirms that a security rule was triggered and the bot operators should change their behavior.

Increased fraud from high activity accounts

The second behavior identified is the use, by bot operators, of numerous "legitimate" accounts to execute credit card fraud. If an account is accessed by Credential Stuffing, that account is now compromised and is more likely to commit fraud. Bot operators use these accessed compromised user accounts numerous times, in order to take advantage of saved credit card, gift card balance, or loyalty points. This combination of increased activity of accessing the account and the increased behavior within it are often a strong indicator of fraudulent activity.

Understanding what bad bots do

Bad bot problem	How it hurts the business	Signs you have a problem	Industries targeted
Price Scraping	Competitors scrape your prices to beat you in the marketplace. You lose business because your competitor wins the SEO search on price. Lifetime value of customers worsens.	Declining conversion rates. Your SEO rankings drop. Unexplained website slowdowns and downtime, usually caused by aggressive scrapers.	All businesses that show prices • E-commerce • Gambling • Airlines • Travel
Content Scraping	Proprietary content is your business. When others steal your content they are a parasite on your efforts. Duplicate content damages your SEO rankings.	Your content appears on other sites. Unexplained website slowdowns and downtime, usually caused by aggressive scrapers.	Similar to Price Scraping, but in addition: • Job boards • Classifieds • Marketplaces • Finance • Ticketing
Account Takeover (aka Credential Stuffing, Credential Cracking)	Stolen credentials tested on your site. If successful, the ramifications are account lockouts, financial fraud, and increased customer complaints affecting customer loyalty and future revenues.	Increase in failed login. Increase in customer account lockouts and customer service tickets. Increase in fraud (lost loyalty points, stolen credit cards, unauthorized purchases). Increase in chargebacks.	Any business with a login page requiring username and password.
Gift Card Balance Checking	Steal money from gift card accounts that contain a balance. Poor customer reputation and loss of future sales.	Spike in requests to the gift card balance page. Increase in customer service calls about lost balances.	E-commerce
Account Creation (aka Account Aggregation)	Free accounts used to spam messages or amplify propaganda. Exploit any new account promotion credits (money, points, free plays).	Abnormal increases in new account creation. Increased comment spam. Drop in conversion rates from new accounts to paying customers.	Messaging platforms • Social media • Dating sites • Communities Sign-up promotion abuse • Gambling

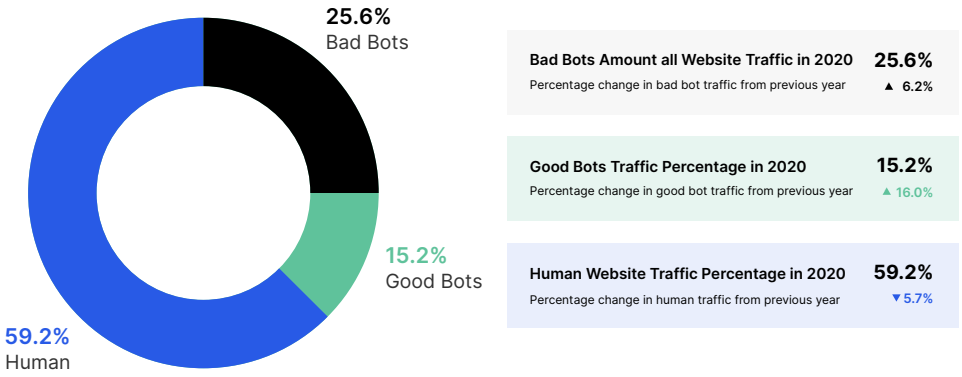
Bad bot problem	How it hurts the business	Signs you have a problem	Industries targeted
Credit Card Fraud (aka Carding, Card Cracking)	Criminals testing credit cards numbers to identify missing data (exp. date, CVV). Damages the fraud score of the business. Increases customer service costs to process fraudulent chargebacks.	Rise in credit card fraud. Increase in customer support calls. Increased chargebacks processed.	Any site with a payment processor • E-commerce • Nonprofit/Charities • Airlines • Travel • Ticketing • Financial • Gambling
Denial of Service	Slows the website performance causing brownouts or downtime. Lost revenue from unavailability of websites. Damaged customer reputation.	Abnormal and unexplained spikes in traffic on particular resources (login, signup, product pages, etc.). Increase in customer service complaints.	All industries
Denial of Inventory	Bots hold items in shopping carts, preventing access by valid customers. Damaged customer reputation because unscrupulous middle men hold all inventory until resold elsewhere.	Increase in abandoned items held in shopping carts. Decrease in conversion rates. Increase in customer service calls about lack of availability of inventory.	Scarce or time-sensitive items • Airlines • Tickets • E-commerce • Healthcare
Scalping (aka Grinchbots, Sneaker Bots, Ticket Bots, Vaccine Bots)	Bots are used to obtain limited-availability and/or preferred goods/services. Damaged customer reputation Slows the website performance causing brownouts or downtime, leading to loss of revenue.	Website slowdowns, potentially even Denial of Service as a side effect of the many requests to the web server Decrease in conversion rates Increase in customer service calls about lack of availability of inventory.	Similar to Denial of Inventory: • Airlines • Tickets • Retail (Sneakers, Consoles, Computer hardware, Limited Edition items) • Healthcare

Executive summary of findings

Bad bot traffic hits an all-time high

In 2020, bad bot traffic has maintained its upwards trend, amounting to 25.6 percent of all traffic, a new record. Combined with good bot traffic, 40.8 percent of internet traffic this past year wasn't human, as human traffic decreased by 5.7 percent to 59.2 percent of all traffic.

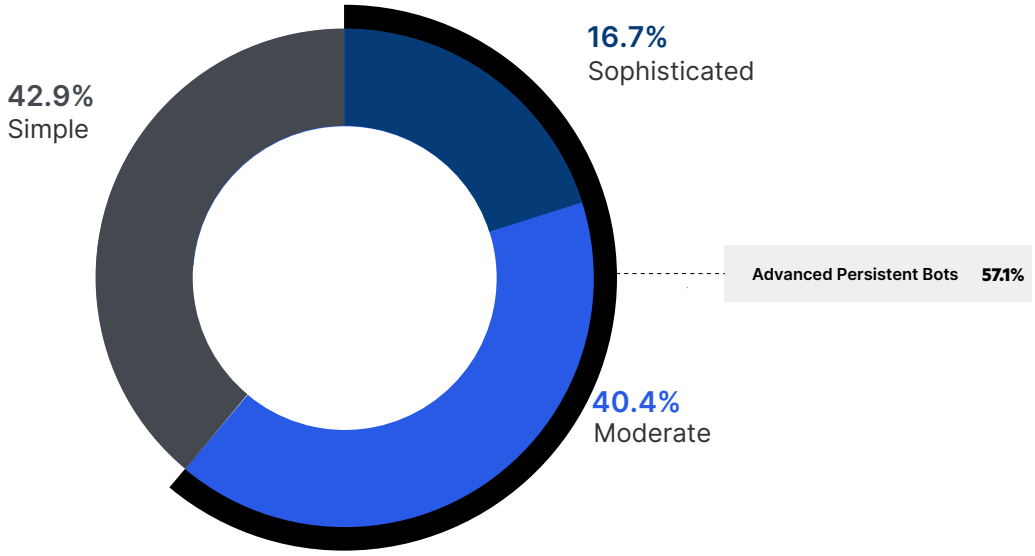
Bad Bot v Good Bot v Human Traffic 2020



Advanced persistent bots are still dominant

Advanced persistent bots (APBs) remain the majority of bad bot traffic, amounting to 57.1 percent. These are a combination of moderate and sophisticated bad bots that are harder to detect and mitigate. They cycle through random IPs, enter through anonymous proxies, change their identities and mimic human behavior.

Bad Bot Sophistication Levels 2020



The bad bot problem is a cross-industry one

As automated threats, or bad bots, are capable of performing various malicious actions, they are affecting all industries. Each industry has its own unique bad bot problem, while some bad bot problems are shared across all industries. Account Takeover, as well as Content and Price Scraping are among the problems that are rampant across many industries.

	Top 5 Industries Bad Bot Traffic %	
1	Telecom & ISPs	45.7%
2	Computing & IT	41.4%
3	Sports	33.7%
4	News	33%
5	Business Services	29.7%

	Top 5 Industries Sophisticated Bad Bot Traffic %	
1	Travel	59.7%
2	Government	15.3%
3	Retail	13.5%
4	Financial Services	11%
5	Food & Beverage	8.6%

Bad bots are shifting towards mobile

While bad bots remain true to the most popular browsers, mostly impersonating Chrome, we are seeing an increase in usage of mobile browsers like Mobile Safari and Mobile Chrome. The preference for mobile doesn't end there, as we observed a growing popularity of attacks being launched from mobile ISPs. Bad bots deployed from Amazon reduced to 10.8 percent.

Bad bots report as mobile user agents (Mobile Safari, Mobile Chrome etc.)	28.1%
Bad bots launched from mobile ISPs	15.1%
Bad bots using Amazon ISP	10.8%

Bad bots around the world

This year, once again, the United States maintained its position at the top list of bad bot traffic originating countries, with 40.5 percent of bad bot traffic coming from the country. This is a significant decline however, of 11.8 percent compared to the previous year.

	Top 5 Bad Bot Traffic By Country	
1	United States	40.5%
2	China	5.2%
3	United Kingdom	4.9%
4	Russia	3.9%
5	Japan	3.4%

	Top 5 Most Attacked Countries	
1	United States	37.2%
2	China	8.3%
3	United Kingdom	6.9%
4	Brazil	4%
5	Japan	3.7%

The bad bot landscape

What is a bad bot?

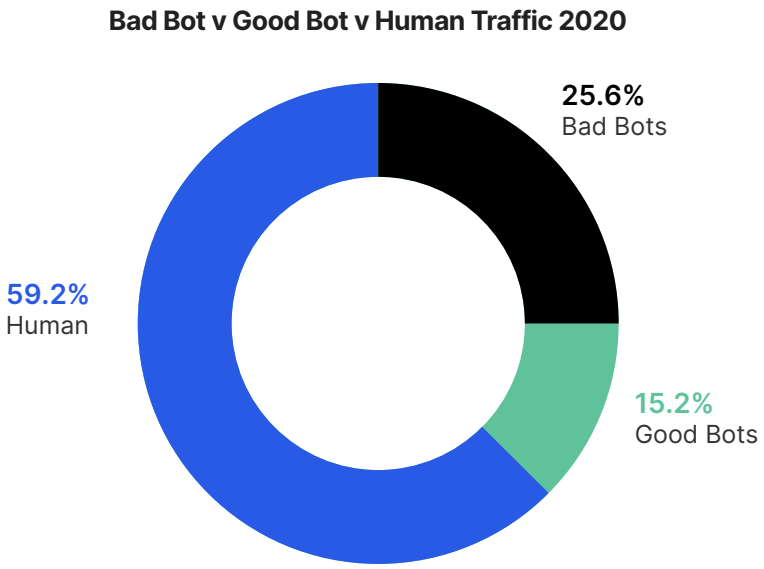
Bad bots are software applications that run automated tasks with malicious intent over the internet. They scrape data from sites without permission in order to reuse it and gain a competitive edge (e.g. pricing, inventory levels, proprietary content). They are used for scalping, the act of obtaining limited availability items for the purpose of reselling at a higher price. The truly nefarious ones undertake criminal activities, such as fraud and outright theft. Credential Stuffing to perform Account Takeover is a prominent tactic of bad bots. The Open Web Application Security Project (OWASP) provides a list of the different bad bot types in its Automated Threat Handbook[8].

How do good and bad bots differ?

In simplistic terms, good bots ensure that online businesses and their products can be found by prospective customers. Examples include search engine crawlers such as GoogleBot and Bingbot that, through their indexing, help people match their queries with the most relevant sets of websites.

Even good bots can be bad news

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 in the sales funnel. This results in lower performance for advertisers. If your website analytics are polluted with bots, any decisions based on the origin of that traffic is potentially flawed. Being able to intelligently separate traffic generated by legitimate human users, good bots, and bad bots is essential for making informed business decisions.

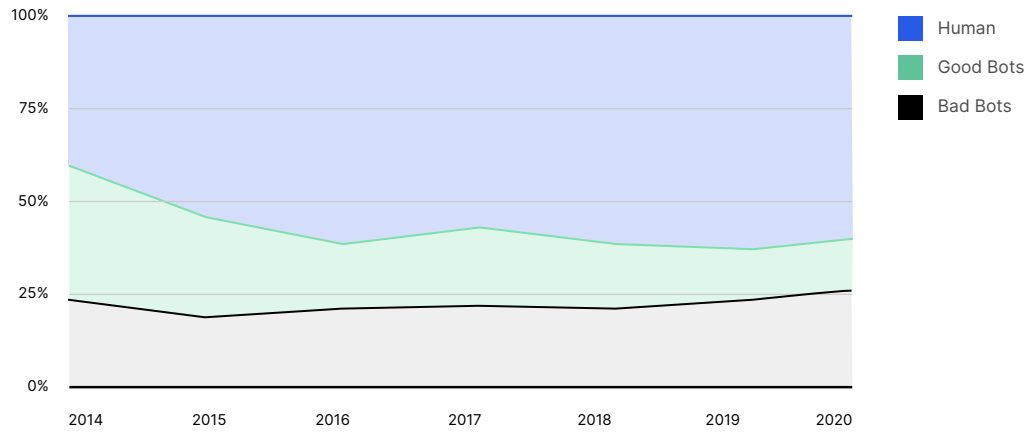


8 https://owasp.org/www-pdf-archive/Automated-threat-handbook.pdf

In 2020, we saw the highest percentage of bad bot traffic since the inception of the bad bot report in 2014. This year, bad bots accounted for 25.6 percent of all website traffic—over a quarter of all traffic is bad bots. That is a 6.2 percent increase over the previous year.

The proportion of good bot traffic has also increased, accounting for 15.2 percent of all traffic. And with both bad and good bots on the rise, the proportion of human traffic is down from 62.8 percent in 2019 to 59.2 in 2020. That is a 5.7 percent decrease from the previous year.

Bad Bot v Good Bot v Human Traffic 2014-2020



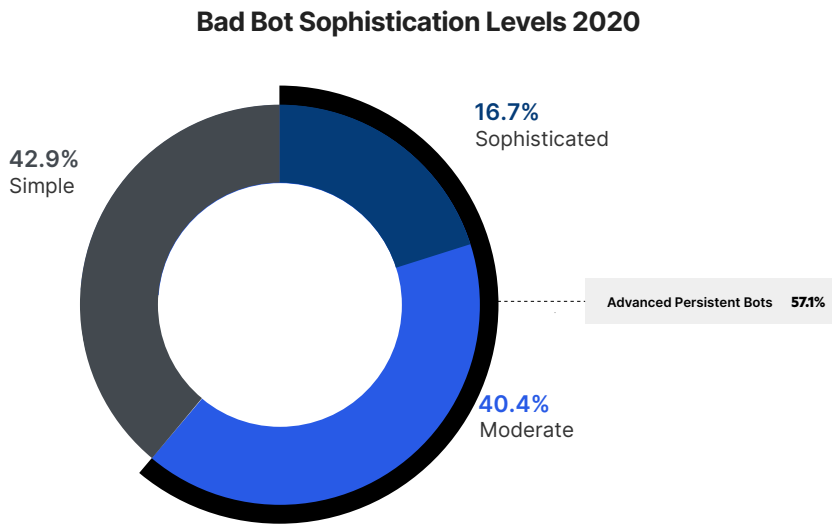
	2014	2015	2016	2017	2018	2019	2020
BAD BOTS	22.8%	18.6%	19.9%	21.8%	20.4%	24.1%	25.6%
GOOD BOTS	36.3%	27.0%	18.8%	20.4%	17.5%	13.1%	15.2%
HUMANS	40.9%	54.4%	61.3%	57.8%	62.1%	62.8%	59.2%

In a year when people were stuck at home during the pandemic and internet usage surged, it is concerning to see that bot operators were also more active than ever and the proportion of automated traffic reached new heights.

Bad bot sophistication levels

Imperva created the following industry-standard system that classifies the sophistication level of the following four bad bot types:

- **SIMPLE** Connecting from a single, ISP-assigned IP address, this type connects to sites using automated scripts, not browsers, and doesn't self-report (masquerade) as being a browser.
- **MODERATE** Being more complex, this type uses "headless browser" software that simulates browser technology—including the ability to execute JavaScript.
- **SOPHISTICATED** Producing mouse movements and clicks that fool even sophisticated detection methods, these bad bots mimic human behavior and are the most evasive. They use browser automation software, or malware installed within real browsers, to connect to sites.
- **ADVANCED PERSISTENT BOTS (APBs)** APBs are a combination of moderate and sophisticated bad bots. They tend to cycle through random IP addresses, enter through anonymous proxies and peer-to-peer networks, and are able to change their user agents. They use a mix of technologies and methods to evade detection while maintaining persistence on target sites.



The broader spectrum of data provided by our Application Security Platform has tipped numbers slightly in favor of simple threats. In previous years, Cloud WAF and Advanced Bot Protection were two seperate systems with separate data sets. Some very simple bad bots that are mitigated at the cloud WAF layer and were usually not a part of Advanced Bot Protection's data set, are now present within it.

While this year we have seen an increase in simple bad bots due to the larger data set obtained from Imperva's Application Security Platform and the addition of Cloud WAF mitigated bots, Advanced persistent bots (APBs) remain the majority of bad bot traffic in 2020.

Advanced persistent bots accounted for 57.1 percent of all 2020 bad bot traffic. APBs, sometimes known as low and slow bots, carry out significant attacks using fewer requests and can even delay requests, all the while staying below request rate limits. This method reduces the 'noise' generated by many bad bot campaigns.

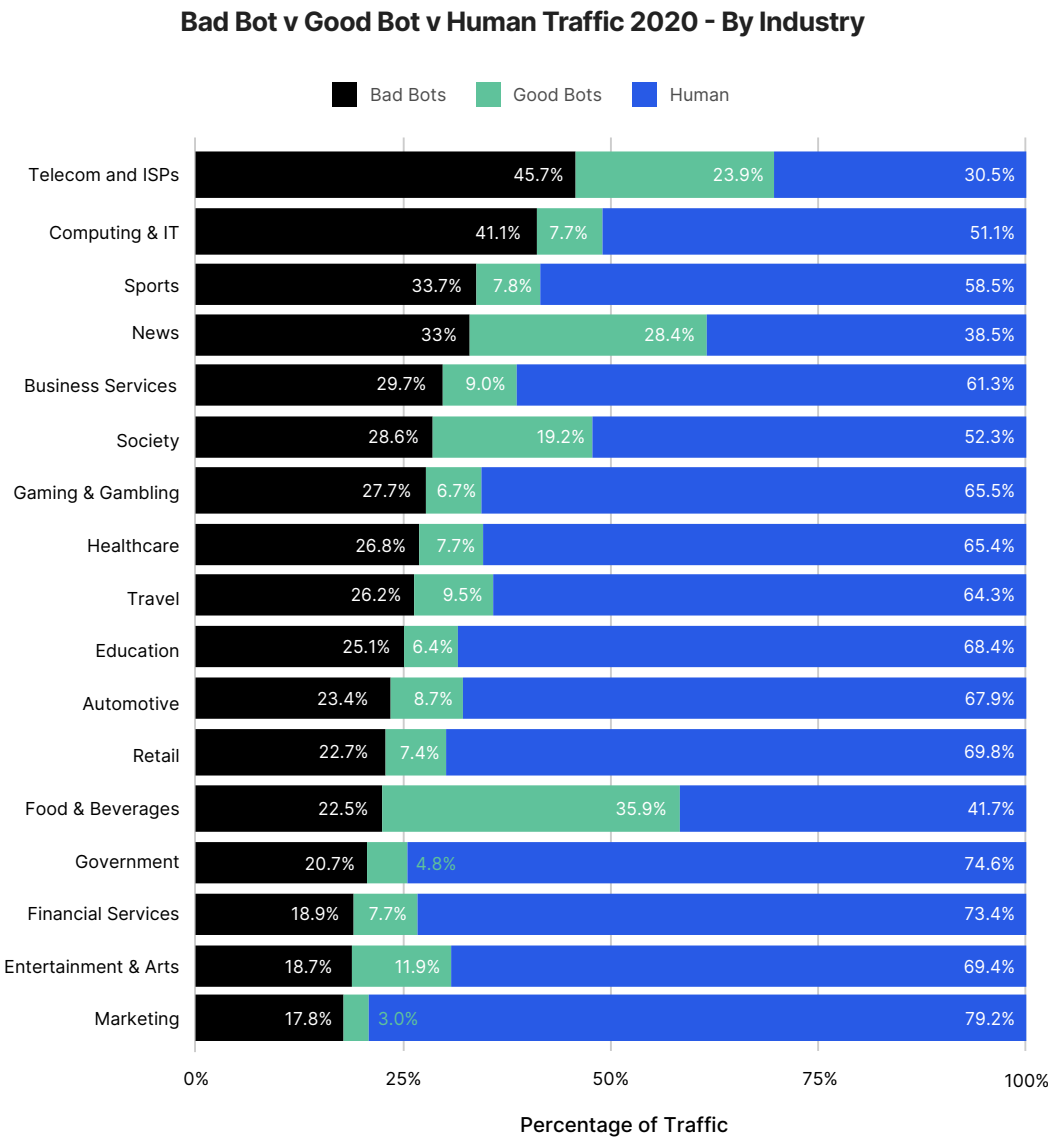
Bad bots by industry

As more organizations add bot protection to their security profile, a larger data set is gathered. For this year's Bad Bot Report, data was collected from 17 industries:

Industry	What businesses are included?	What bad bots do?
Automotive	Manufacturers, Dealerships, Vehicle Marketplaces	Price Scraping, Data Scraping, Inventory Checking
Business Services	Real Estate, Third Party Vendors Like E-Commerce Platforms, CRM Systems, Business Metrics	Attacks on the API Layer, Data Scraping, Account Takeover
Computing & IT	IT Services, IT Providers, Services And Technology Providers	Account Takeover, Scraping
Education	Online Learning Platforms, Schools, Colleges, Universities	Account Takeover for Students and Faculty, Class Availability, Scraping Proprietary Research Papers and Data Proprietary Research Papers and Data
Entertainment & Arts	Streaming Services, Ticketing Platforms, Production Companies, Venues	Account Takeover, Price Scraping, Inventory Checking, Scalping
Financial Services	Banking, Insurance, Investments, Cryptocurrency	Account Takeover, Carding, Card Cracking, Custom Content Scraping
Food & Beverages	Food Delivery Services, Online Grocery Shopping, Food & Beverage Brand Sites	Credit Card Fraud, Gift Card Fraud, Account Takeover
Gaming & Gambling	Online Gaming, Casinos, Sport Betting	Account Takeover, Odds Scraping, Account Creation for Promotion Abuse

Industry	What businesses are included?	What bad bots do?
Healthcare	Health services, pharmacies	Account Takeover, Content Scraping, Helpful bots - vaccine availability, Inventory Checking, vaccine appt availability
Government	Law & Government Websites, Citizen Services, States, Municipalities, Metropolitans	Account Takeover, Data Scraping of business registrations listings, Voter Registration
Marketing	Marketing Agencies, Advertising Agencies	Custom Content Scraping, Ad Fraud, Denial of Service, Skewing
News	News Sites, Online Magazines	Custom Content Scraping, Ad Fraud, Comment Spam
Retail	E-Commerce, Marketplaces, Classifieds	Denial f Inventory (Grinchbots, Sneakerbots Etc.), Credit Card Fraud, Gift Card Fraud, Account Takeover, Data and Price Scraping, Skewing
Society	Nonprofits, Faith and Beliefs, Romance And Relationships, Online Communities, LGBTQ, Genealogy	Data Scraping, Account Takeover, Account Creation, testing stolen credit cards on donation pages
Sports	Sports updates, news, live score services	Data Scraping (Live Scores, Odds Etc.)
Telecom & ISPs	Telecommunications Providers, Mobile ISPs, Hosting Providers	Account Takeover, Competitive Price Scraping
Travel	Airlines, Hotels, Holiday Booking	Price and Data Scraping, Skewing of Look-To-Book Ratio, Denial of Service, Price Scraping, Account Takeover

The following chart provides a breakdown of traffic for each industry. It enables a deeper insight into the bot problem that each is suffering from.



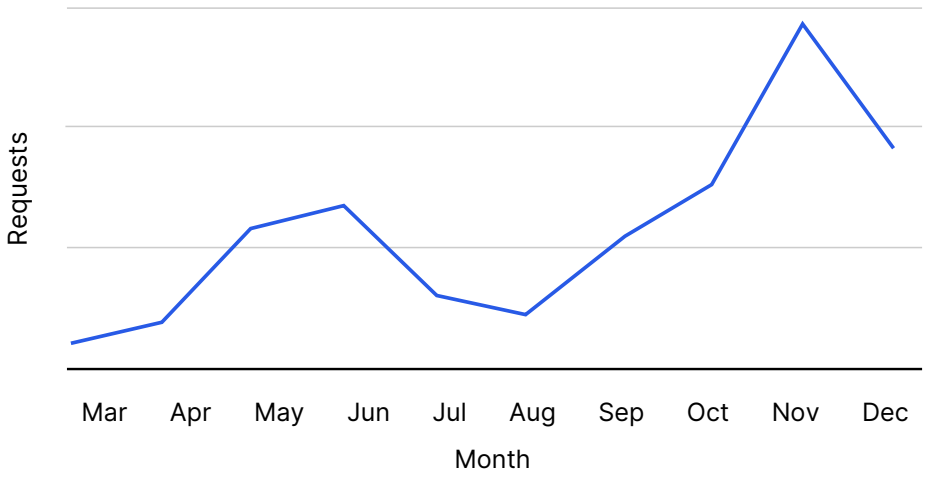
TELECOM & ISPs sit at the top, with 45.7 percent of their traffic originating from bad bots. This includes mobile ISPs, residential ISPs, hosting providers, and more. Account Takeover, as well as Price and Data Scraping by competitors are the main concerns for the industry.

NEWS websites had 33 percent of traffic comprising bad bots. The main concerns for the industry are ad fraud, Account Takeover, and scrapers stealing articles and other proprietary content as well as comment spam.

SOCIETY, with 28.6 percent bad bot traffic, includes many nonprofit organizations. Bots use their donation pages to test stolen credit card numbers, causing great trouble and a financial burden that many nonprofits cannot afford to endure.

TRAVEL, regardless of the drastic decline in holiday bookings and flight reservations due to the global pandemic, had 26.2 percent of traffic comprising bad bots. Looking at the trendline for sophisticated bad bot traffic to travel websites reveals early signs of reawakening in the industry, as traffic spiked by 538 percent between August and November. The bot problem of this industry is very complicated. Prices are being scraped not only by direct competitors, but also by third-party players in the expansive travel ecosystem. Unauthorized online travel agencies (OTAs), competitors, price aggregators, and metasearch sites use sophisticated scraping bots to abuse the business logic of booking engines. Querying for any ticket they can sell, they skew look-to-book ratios, increase GDS transaction costs, and are responsible for site slowdowns and downtime—causing customer dissatisfaction during disruptions. Airlines specifically, are suffering from Account Takeover issues as bad bot operators attempt to get into user accounts and empty them of accumulated air-mile balances.

Sophisticated Bad Bot Traffic on Travel Websites



EDUCATION had 25.1 percent of its traffic comprising bad bots. The global pandemic has forced most if not all educational institutions to increase their online presence. From live classes to recordings and online resources. Bad bots are used by malicious operators in order to scrape research papers, look for class availability and access user accounts (Account Takeover). In addition, the popularity of online learning platforms has skyrocketed as people were looking for new career paths, learning new hobbies or just enriching their knowledge. With an abundance of platforms available, competition is fierce, thus price and content scraping are common.

RETAIL saw bad bots accounting for 22.7 percent of traffic. Price Scraping by competitors and third parties, Content Scraping, Inventory Fraud (Grinchbots, Sneakerbots, etc.), Account Takeovers, Credit Card Fraud and Gift Card abuse are a few of the bad bot problems that the retail industry suffers from. We saw an increase of 28 percent in traffic to retail websites shortly after stay-at-home orders were given worldwide, which made inventory hoarding much more appealing. In addition, bad bots have aggressively targeted the gaming hardware market in the second half of the year and throughout the holiday season.

HEALTHCARE has seen 26.8 percent of its traffic comprising bad bots in 2020. The main concerns in the industry are Account Takeover attacks as well as data theft and the recent vaccine bots. According to a National Cyber Awareness report from May 2020, cybersecurity agencies have been investigating large-scale password spraying attacks on healthcare-related organizations in several countries including the US and the UK[9]. Helpful bots that are checking for data to understand regional availability of vaccines are also being deployed.

FINANCIAL SERVICES had 18.9 percent of traffic comprising bad bots. Such companies typically suffer from bad bots attempting to access user accounts using Credential Stuffing or Credential Cracking, Credit Card Fraud and custom content theft such as frequently changing interest rates.

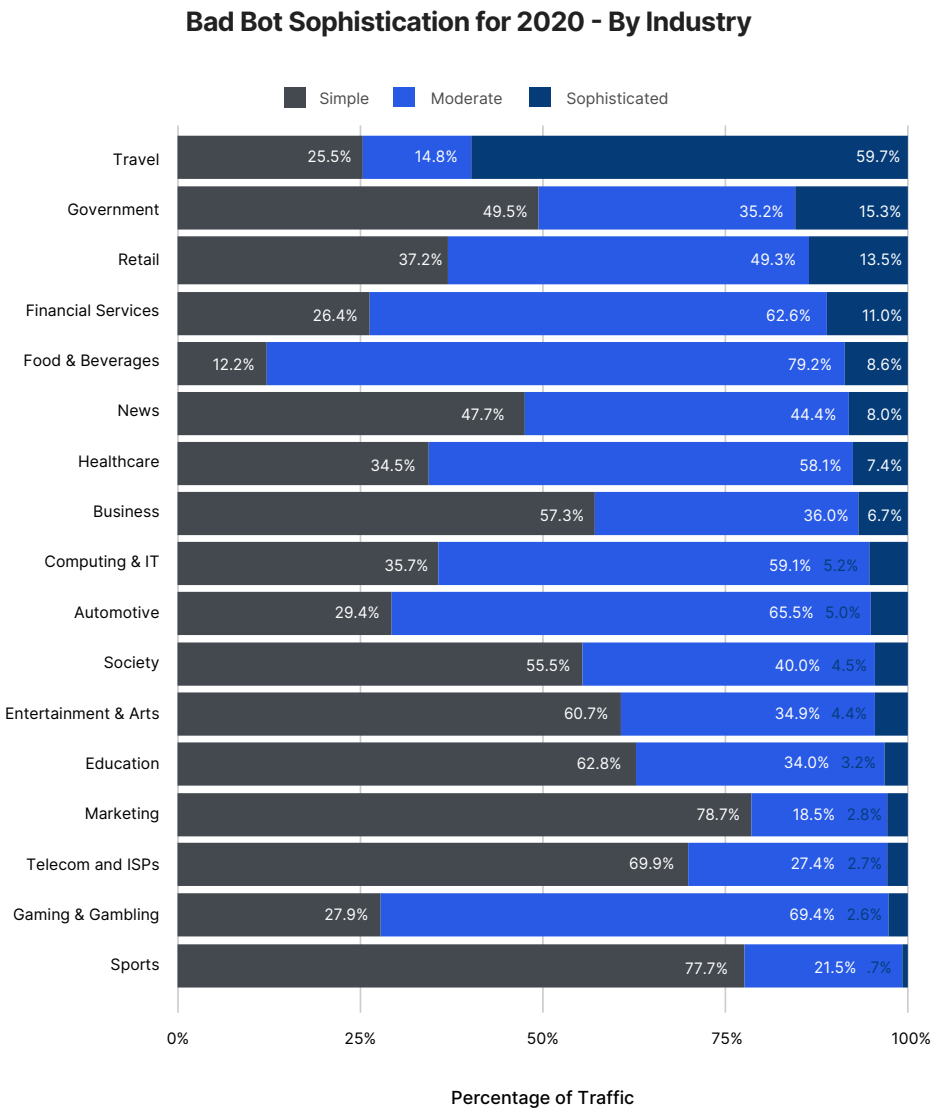
GOVERNMENT, with 20.7 percent of bad bots, is interested in protecting business registration listings from scraping bots, and in stopping election bots from interfering with voter registration accounts.

9 https://www.us-cert.gov/ncas/alerts/AA20126A

Bad bot sophistication by industry

Through dissecting bad bot sophistication levels by industry, we gain a new perspective of the threat landscape as positioning changes from the previous chart, to reveal a different picture. From this perspective, travel, government, retail, financial services, gaming & gambling, and business services saw the highest proportions of sophisticated bad bot traffic throughout 2020.

It is essential to understand that the volume of bad bot traffic doesn't necessarily align with the sophistication of these bot attacks. For example, a sophisticated bad bot may be able to achieve its goal while performing fewer requests than simpler bad bots.



Account Takeover remains a significant threat

The prevalence and sophistication of Account Takeover attacks is constantly rising. If your business has a login page—it is under continuous Credential Stuffing and Credential Cracking attacks. With billions of stolen credentials available at a price, Account Takeover (aka ATO) is a thorn in the side of every business.

Account Takeover attacks by the numbers

34%	Percentage of all login attempts that are malicious bots.etc.)
16%	Average percentage of time a website is subjected to Account Takeover attacks
45%	Account Takeover attacks that originated from the USA

Top industries targeted by Account Takeover attacks

Computing & IT
Travel
Retail
Financial Services
Entertainment
Telecom & ISP

Top countries that originate Account Takeover attacks

USA
Brazil
China
Russia
United Kingdom

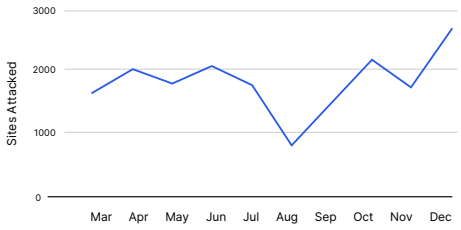
Account Takeover bots impersonate popular browsers

Many Account Takeover attacks are launched from proprietary bot engines or tools, but the majority (47.2 percent) is still trying to impersonate as a legitimate browser, mostly Chrome.

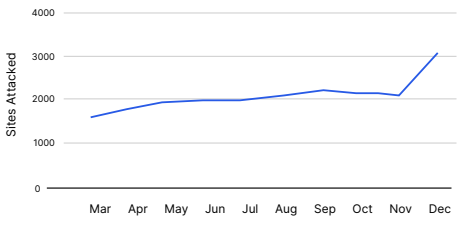
Account Takeover attacks spiked in November and December

More websites were attacked as 2020 drew to a close. Spikes in attacks to Financial Services websites (51 percent increase), as well as Telecom & ISPs (49 percent increase) rose towards the end of 2020.

Account Takeover Attacks on Financial Services



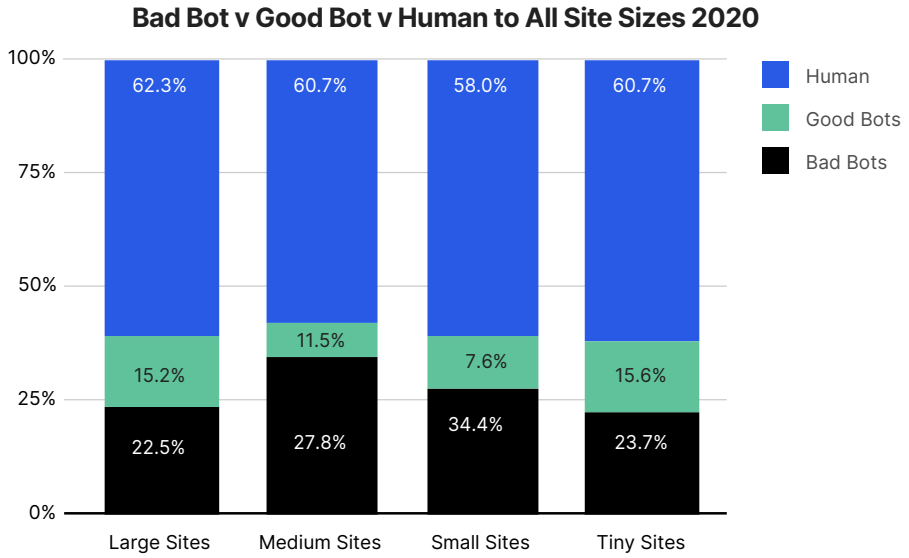
Account Takeover Attacks on Telecom & ISPs



Bad bot traffic by website size

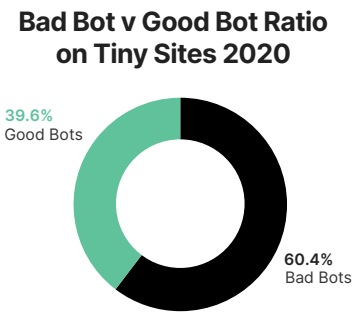
There are differences in bot traffic by size of website. All sites were sorted by the amount of requests, from highest to lowest and then split by the following percentages of all traffic:

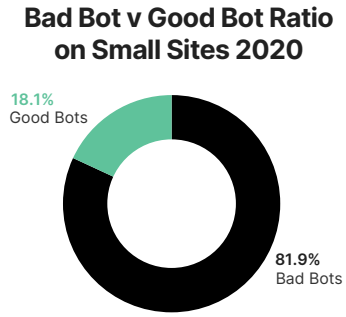
Tiny = lowest 50% of traffic
Small = next 25% of traffic
Medium = next 15% of traffic
Large = top 10% of traffic

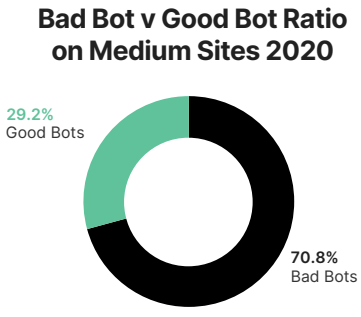


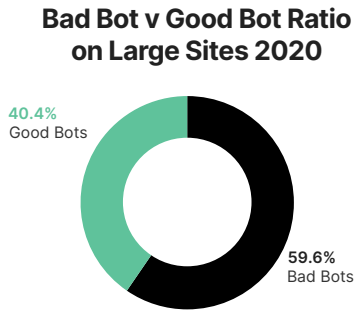
Bad bot traffic volume has gone up for almost every website size during 2020, with the only exception being the tiny sites. This year, small websites had the highest proportion of bad bot traffic, at 34.4 percent.

The following four charts show the bad to good bot traffic ratio for large, medium, small, and tiny sites. Small sites saw the highest ratio of bad bots (81.9 percent) to good bots (18.1 percent). The trend which began last year, of bad bot traffic overtaking good bot traffic on all website sizes continues for the second year in a row.





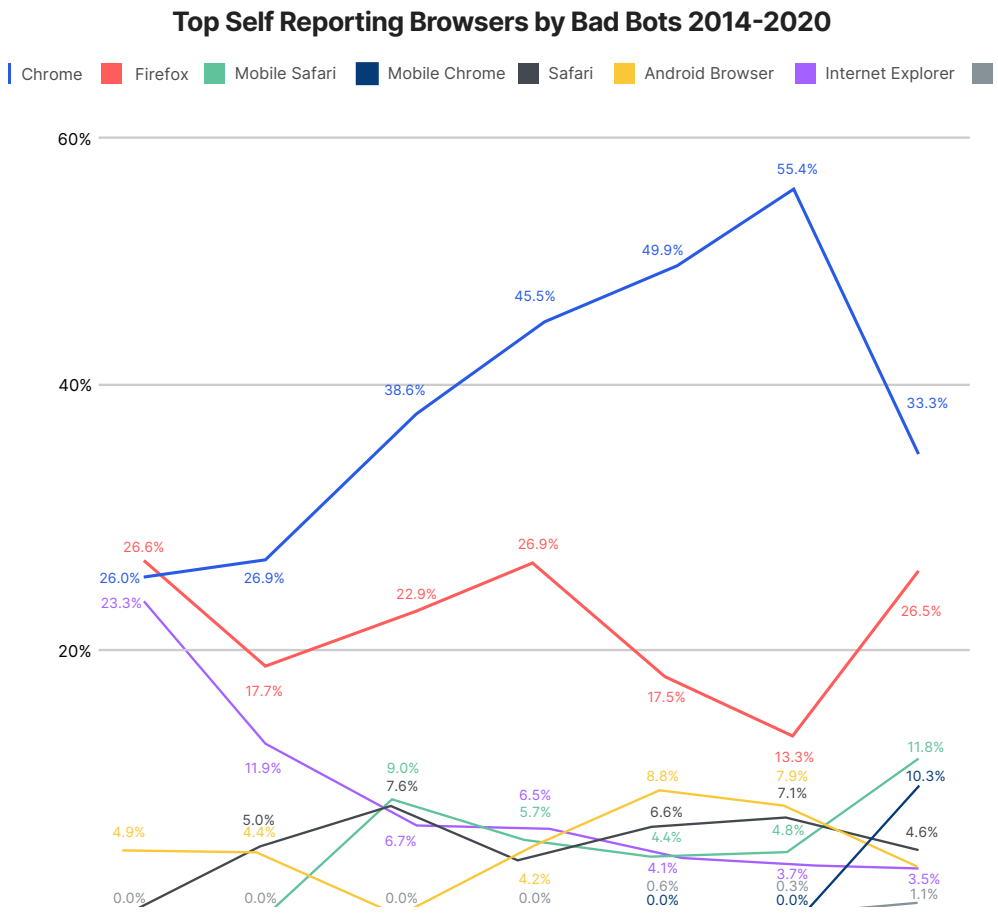


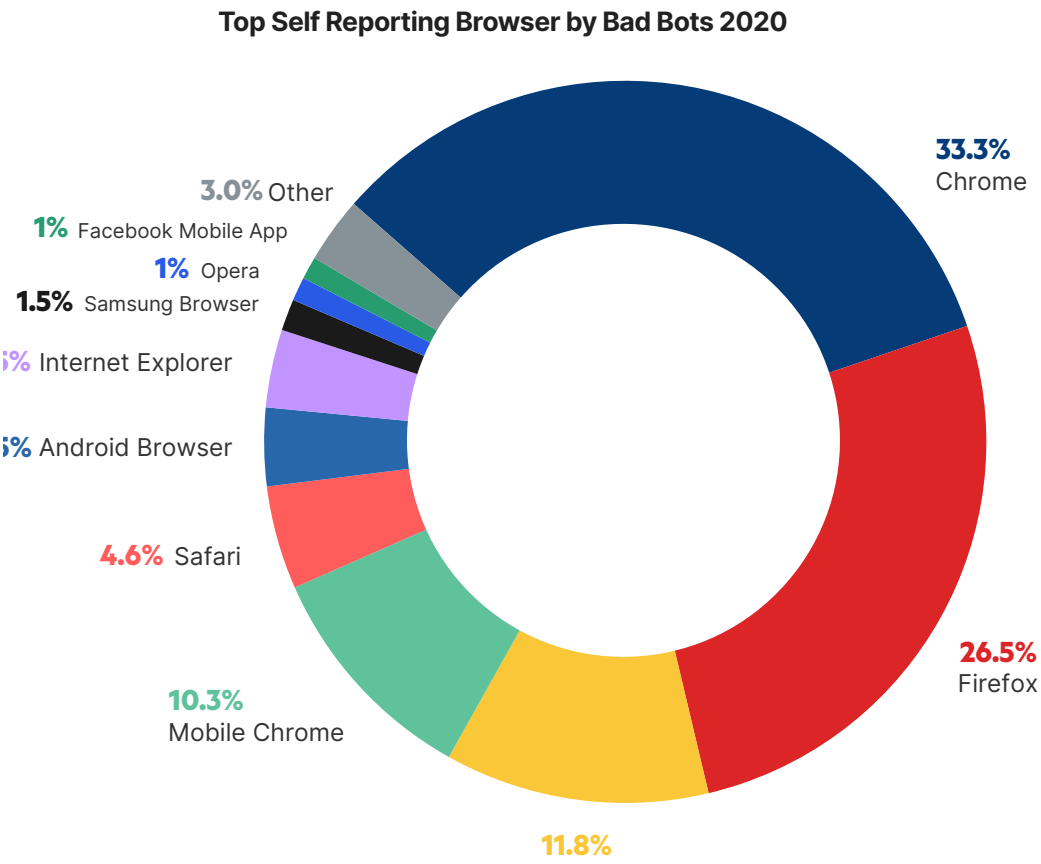


Bad bot identity: Chrome drops in popularity, still a favorite

In order to avoid being detected, bad bots are typically masquerading as legitimate users by reporting their user agent as a web browser or mobile device. They also want to make sure they use a web browser or mobile device that is common and popular among legitimate users, to not raise suspicions.

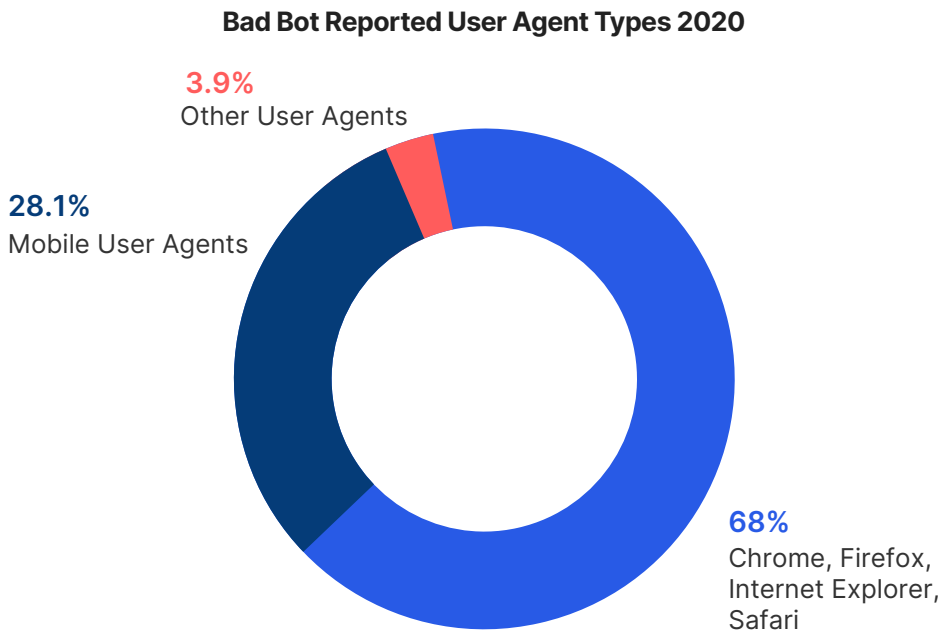
In 2020, Chrome remains the most popular fake identity selection used by bad bots, maintaining its dominance in recent years. Yet, numbers have shifted slightly to open up the landscape for competition. Chrome dropped from being over half of the traffic (55.4 percent) in 2019 to just a third (33.3 percent) in 2020. Firefox on the other hand, is regaining popularity, going back to 2014 levels, with 26.5 percent of traffic. Another trend this year is a rise in mobile browser popularity among bad bots, with Mobile Safari leading the pack (11.8 percent) and Mobile Chrome following closely (10.3 percent).

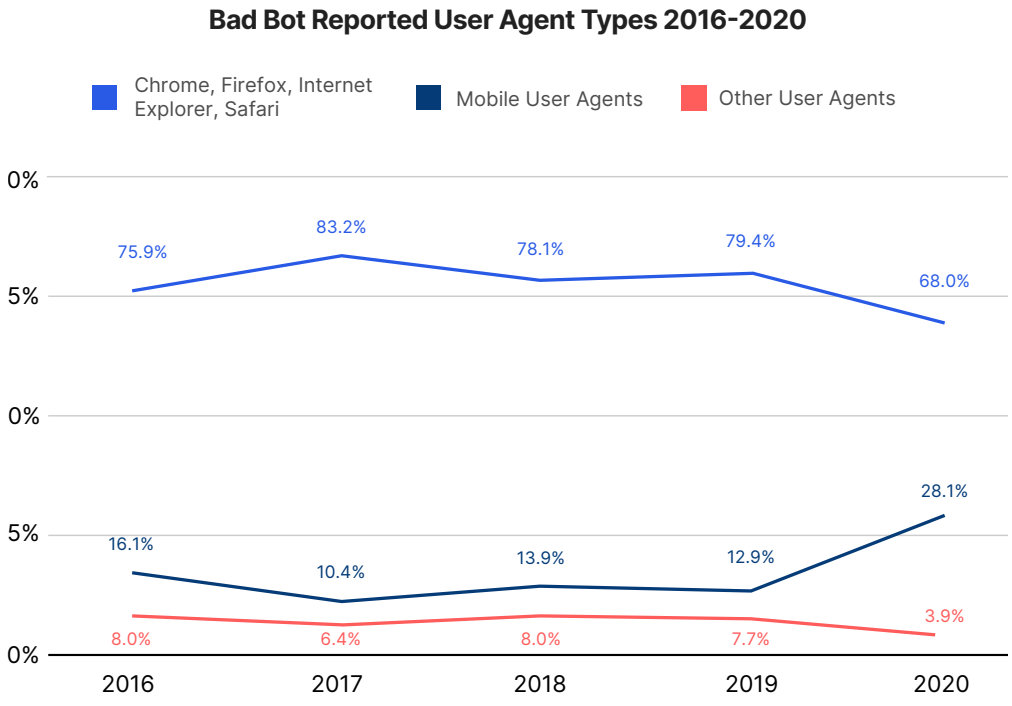




Mobile bots on the rise

The majority of bad bots (68 percent) are self-reporting as either Chrome, Firefox, Safari or Internet Explorer. This is lower than the previous year (79.4 percent), as mobile user agents gain popularity, with a substantial rise from 12.9 percent in 2019 to 28.1 percent in 2020. The remainder of bad bot traffic, 3.9 percent, has reported themselves as other user agents like Google Search App or QQ and WeChat browsers.

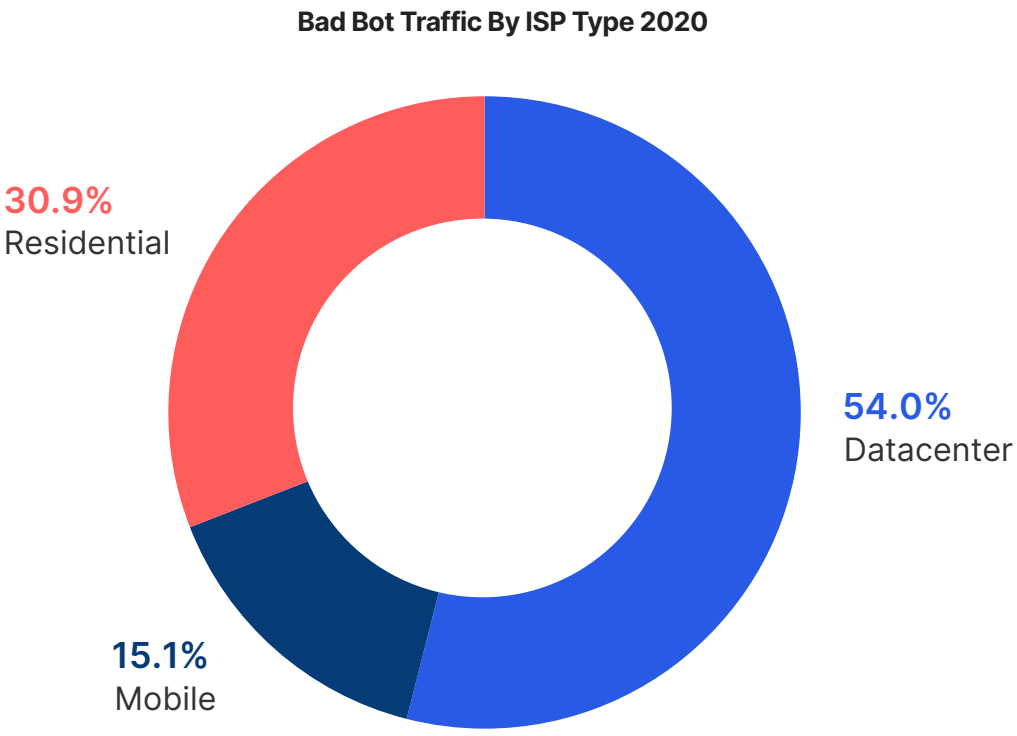




Mobile ISPs playing a bigger role

Data centers are still responsible for the majority of bad bot traffic, with 54 percent of bad bots originating from them. That is a significant decrease from last year (70 percent). The trend of bad bots originating from residential ISPs that has been going for four years in a row, continued this year, going up from 27.8 percent to 30.9 percent in 2020.

Bad bot traffic from mobile ISPs increased significantly in 2020, accounting for a staggering 15.1 percent of traffic. That is a 556.5 percent increase from 2019 (2.3 percent).



Amazon remains a top source of bad bot traffic

Bad bots were launched from 3,402 ISPs during 2020.

- With more ISPs being used to launch bad bot attacks, Amazon dropped from 11.6 percent in 2019 to 10.8 percent in 2020
- For the first time, a mobile ISP claims the second spot. Smart Communications had 4.39 percent of bad bot traffic originating from their servers
- Another first, a residential ISPs claims the fourth spot. Spectrum had 3.58 percent of bad bot traffic originating from their servers

Residential is still growing in popularity

As the residential ISP market expands, it provides attackers with more options to launch bad bots from when they find that their data center traffic is blocked. It also allows them to be better disguised when masquerading as legitimate users. In addition, many mobile ISPs are adding residential service and vice versa. Essentially, what that means is the probability of more bot attacks being launched from residential and mobile ISPs is predicted to increase.

Top 10 Bad Bot Originating ISPs in 2020

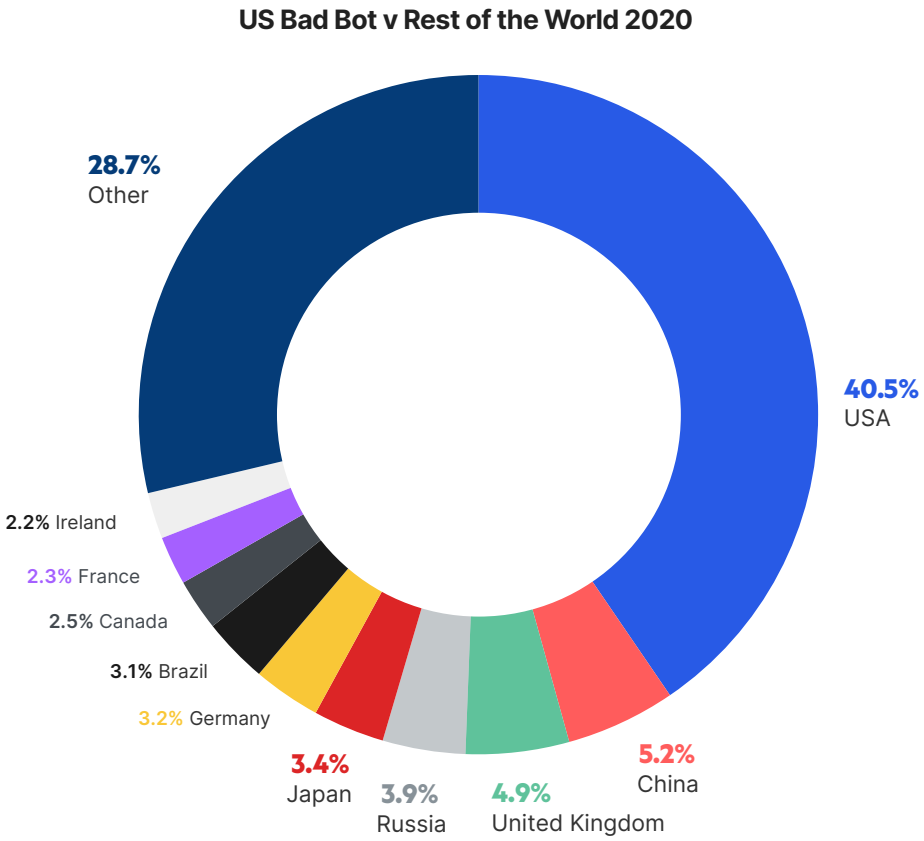
Rank	ISP	% of traffic
1	Amazon.com	10.80%
2	Smart Communications	4.39%
3	China Telecom	4.21%
4	Spectrum	3.58%
5	Host Europe GmbH	2.57%
6	Comcast Cable	2.43%
7	Dedibox SAS	2.11%
8	Digital Ocean	2.54%
9	AT&T U-verse	1.81%
10	Hangzhou Alibaba Advertising Co.,Ltd.	1.57%

Top 10 Mobile ISPs

Rank	ISP	% of traffic
1	Smart Communications	4.39%
2	China Unicom Liaoning	1.01%
3	PT Telkom Indonesia	0.70%
4	China Mobile Guangdong	0.68%
5	Safaricom	0.66%
6	Korea Telecom	0.66%
7	China Unicom Beijing	0.47%
8	China Telecom Shanghai	0.40%
9	Turk Telekom	0.31%
10	ER-Telecom	0.27%

Where bad bots originate

- The United States maintains its reign at the top of the list for the seventh consecutive year. It does however continue the trend of decline. It went from 53.4 percent in 2018, to 45.9 percent in 2019 and 40.5 percent in 2020
- China comes in second, with an increase in volume to 5.2 percent
- The United Kingdom was the origin of 4.9 percent of bad bot traffic
- Russia's volume of traffic increased to 3.9 percent
- New to the top 10, Japan had 3.4 percent of bad bot traffic originating from it, while Brazil had 3.1 percent



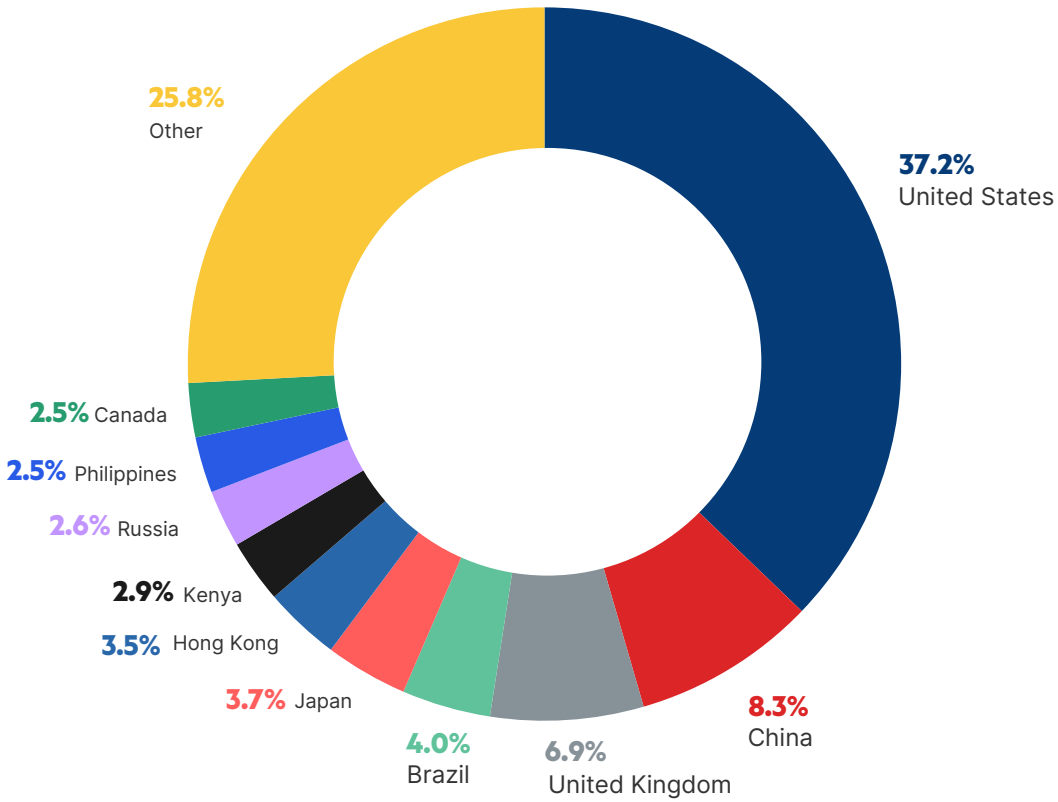
The United States and China are the most attacked countries

It appears that on many occasions, bad bots are launched from the same country they are targeting. The United States was the most attacked country by bad bots in 2020, as traffic targeting it amounted to 37.2 percent of all bad bot traffic. China was the second most attacked country, targeted by 8.3 percent of all bad bot traffic.

Top 10 Most Attacked Countries by Bad Bots

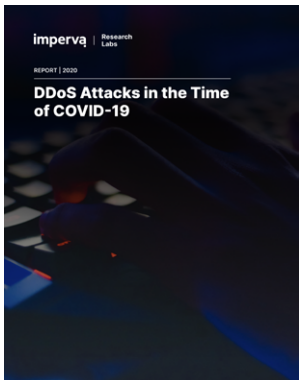
1		United States	6		Hong Kong
2		China	7		Kenya
3		United Kingdom	8		Russia
4		Brazil	9		Philippines
5		Japan	10		Canada

Top Targeted Countries by Bad Bots 2020



Imperva Threat Research Lab

Threat Research



DDoS Attacks In The Time Of Covid 19

Key Finding

Application DDoS attacks increased in intensity by almost 80%

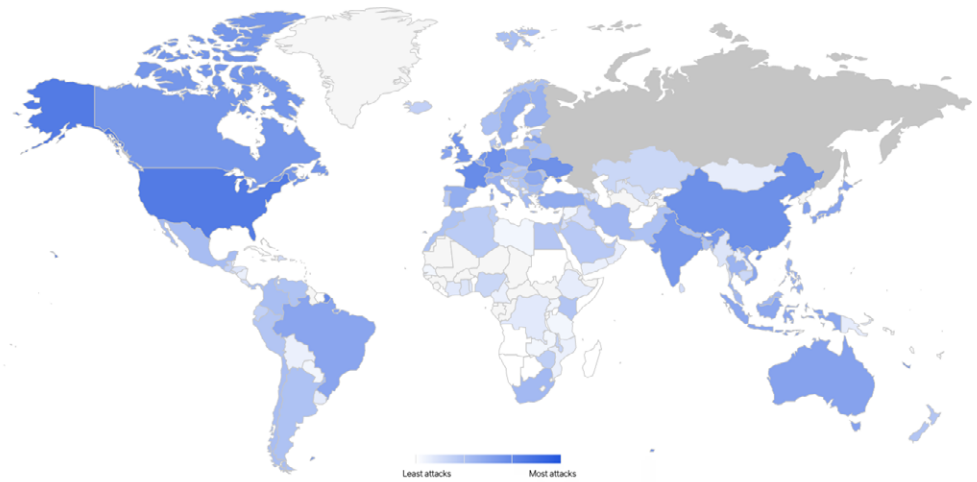
The State of Vulnerabilities in 2020

Key Finding

XSS was the most dominant category of web-related vulnerabilities (28%)

Cyber Threat Index

The Cyber Threat Index is a monthly measurement and analysis of the global cyber threat landscape across data and applications. It provides an easy-to-understand score to track cyber threat level consistently over time, as well as observe trends. The data is (when applicable) also analyzed by industry and by country, to provide further analytics and insights.



Recommendations

Bots are on your website every day, and attack characteristics are becoming more advanced and nuanced over time. How should businesses go about protecting themselves? Unfortunately, every site is targeted for different reasons, and usually by different methods, so there is no one-size-fits-all bot solution. But there are some proactive steps you can take to start addressing the problem today.

Recommended actions for detection of bad bot activity

1. PLAN AHEAD WHEN UPDATING YOUR WEBSITE:

a. MARKETING CAMPAIGNS BRING MORE BOTS
For example - LAUNCHING A LIMITED QUANTITY, HIGH-DEMAND PRODUCT. Whether it is a highly sought after pair of sneakers or a new generation gaming console, announce a date and time for a coveted product launch, and bots will be there to get their hands on it first. Make sure that you are prepared to handle the high volume of traffic that is going to include a high ratio of sophisticated bots trying to scoop up the products and deny your customers access.

b. NEW FUNCTIONALITIES BRING MORE BOTS: Some website functionalities are highly exploitable by bad bots. Adding login functionality opens up the chances of Credential Stuffing and Credential Cracking attacks. Adding a checkout form increases the chances of credit card fraud (Carding/Card Cracking). Adding gift card functionality invites bots to commit fraud. Make sure that these pages have extra security measures and a more strict ruleset.

2. BLOCK OR CAPTCHA OUTDATED USER AGENTS/BROWSERS:
The default configurations for many tools and scripts contain user-agent string lists that are largely outdated. This won't stop the more advanced attackers, but it might catch and discourage some. The risk in blocking outdated user agents/browsers is very low; most modern browsers force auto-updates on users, making it more difficult to surf the web using an outdated version.

We recommend you block or CAPTCHA the following browser versions:

	Block End of Life more than 3 years	**CAPTCHA** End of Life more than 2 years
Chrome version	**<64**	**<72**
Firefox version	**<64**	**<72**
Safari version	**<64**	**<72**
Internet Explorer version	**<64**	**<72**

3. BLOCK KNOWN HOSTING PROVIDERS AND PROXY SERVICES:
Even if the most advanced attackers move to other, more difficult to block networks, many less sophisticated perpetrators use easily accessible hosting and proxy services. Disallowing access from these sources might discourage attackers from coming after your site, API, and mobile apps. Consider blocking traffic from these data centers: *Host Europe GMBH, Dedibox SAS, Digital Ocean, OVH SAS & Choopa, LLC*.

4. BLOCK ALL ACCESS POINTS:
Be sure to protect exposed APIs and mobile apps—not just your website—and share blocking information between systems wherever possible. Protecting your website does little good if backdoor paths remain open.

5. CAREFULLY EVALUATE TRAFFIC SOURCES:
Monitor traffic sources carefully. Do any have high bounce rates? Do you see lower conversion rates from certain traffic sources? They can be signs of bot traffic.

6. INVESTIGATE TRAFFIC SPIKES:
Traffic spikes appear to be a great win for your business. But can you find a clear, specific source for the spike? One that is unexplained can be a sign of bad bot activity.

7. MONITOR FOR FAILED LOGIN ATTEMPTS:
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.

8. MONITOR INCREASES IN FAILED VALIDATION OF GIFT CARD NUMBERS:
An increase in failures, or even traffic, to gift card validation pages can be a signal that bots such as GiftGhostBot are attempting to steal gift card balances.

9. PAY CLOSE ATTENTION TO PUBLIC DATA BREACHES:
Newly stolen credentials are more likely to still be active. When large breaches occur anywhere, expect bad bots to run those credentials against your site with increased frequency.

10. EVALUATE A BOT PROTECTION SOLUTION:
The bot problem is an arms race. Bad actors are working hard every day to attack websites across the globe. The tools used constantly evolve, traffic patterns and sources shift, and advanced bots can even mimic human behavior. Hackers who use bots to target your site are distributed around the world, and their incentives are high. In early bot attack days, you could protect your site with a few tweaks; this report shows that those days are long gone. Today, it's almost impossible to keep up with all of the threats on your own.

Industry analysts agree, which is why Gartner has added bot defense as a core requirement for WAF and CDN vendors. Your defenses need to evolve as fast as the threats, and to do that you need dedicated support from a team of experts.

About Imperva Application Security

The Imperva Application Security platform mitigates risk for your business with full-function defense-in-depth, providing protection wherever you choose to deploy - in the cloud, on-premises, or via a hybrid model.

The platform combines best-of-breed solutions that bring defense-in-depth to a new level:

- 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.
- 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.

Through App Protect, our unique licensing model, you can deploy Imperva Application Security how and when you need it. App Protect helps protect your applications wherever they live — in the cloud, on-premises or in a hybrid configuration.

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