distil networks

Blue Cube
Intelligent Protection

# 2019 BAD BOT REPORT

## The Bot Arms Race Continues

# Table of Contents

# About the Bad Bot Report

Distil Networks' 2019 Bad Bot Report investigates the daily attacks that sneak past sensors and wreak havoc on websites. It's based on 2018 data collected from Distil Networks' global network and includes hundreds of billions of bad bot requests anonymized over thousands of domains. Our goal is to offer guidance about the nature and impact of automated threats to those of you on the frontlines of website security.

What makes this report unique is its focus on bad bot activity at the application layer (layer 7 of the OSI model). Automated application layer attacks differ from volumetric DDoS attacks, the latter of which manipulate lower level network protocols.

Bad bots interact with applications in the same way a legitimate user would, making them harder to prevent. They enable high-speed abuse, misuse, and attacks on your websites and APIs. They enable 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 and digital ad fraud, spam, transaction fraud, and more.

# The Business of Bots is Money

While it's well known that bots were used to exploit social media sites in an attempt to influence political dialogue and elections, the real motivation behind the majority of bad bots is more simple—money.

While the goal of each bot operator might be different depending on their industry, bots are the tool of choice and are vital to their success. There is an ecosystem within many industries that rely on bots for survival. Without their use, many such operators would struggle to compete. In many cases, deploying bad bots is an essential business practice.

Every industry has its own bad bot problem and ecosystem of bot operators. Some of these include:

- **Airlines**
  There is an ecosystem of online travel agents, aggregators, and competitors that use bots to scrape content—including flight information, pricing, and seat availability—while criminals attempt to fraudulently access user accounts that contain loyalty program awards and credit card information.[1]
- **Ecommerce**
  Competitors use bad bots to aggressively scrape pricing and inventory information. Criminals use them to commit fraud by stealing gift card balances and to access user accounts and credit card information.
- **Event Ticketing**
  Brokers, scalpers, hospitality agencies, and corporations use bad bots to check for ticket availability and to purchase available seats to resell on secondary markets. Criminals access user accounts to steal tickets and credit card information. [2]

But for any business whose website, mobile app, or API is the unfortunate target of malicious bots, the story is the complete opposite. Not only does it have to deal with the competitive pricing pressure resulting from the scraping bots, but it has to maintain infrastructure uptime and redundancy so that real customers aren't inconvenienced. In addition, they also suffer from skewed decision-making metrics because their web traffic has been polluted by bad bots.

To add insult to injury, the financial investment sector also deploys bots to scrape for information such as inventory levels and pricing data. Sometimes known as alternative data, this information is used by hedge funds to make investment decisions. A recent report estimated that 5% of all web traffic is attributable to investment-scraping bots.[3]

[1] Distil Research Lab: Threat Research: How Bots Affect Airlines

[2] Distil Research Lab: Threat Research: How Bots Affect Ticketing

[3] Web Scraping for Investments (Published by Opimas (Feb 2019))

To understand the scale of the bot problem, the report also estimated that hedge funds are expected to pay $2B in 2020 to collect and store data that was scraped from websites.

> *"Hedge funds are expected to pay $2B in 2020 to collect and store data that was scraped from websites."*

This clearly shows the business value of running bad bots. So not only can competitors use them to beat you in the marketplace, and criminals can use them to defraud your business, but the investment community also uses them to potentially punish your business performance based on any gathered information. It would be wrong to consider bots as being benign.

## The Data Breach Problem Escalates the Bad Bot Volume

The increasing volume of stolen credentials from data breaches is creating a worsening bot problem for any online business having a login page. Bots are used by criminals to test the viability of stolen credentials. Every new data breach sees an increased availability of credentials and leads to higher volumes of bad bot traffic. With over 14 billion credentials stolen since 2013, the problem is already significant—and only getting worse.


Data records lost or stolen since 2013

https://breachlevelindex.com/
(April 2019)

## Global Legislation Still Focused on Ticketing

In the past few years, governments in the US; UK; Ontario, Canada; New South Wales, Australia; and New Zealand have either recently enacted legislation to prevent bots in ticketing, or they plan to in the near future. And yet there is still very limited enforcement. And what about all the other industries suffering from bad bot abuse?

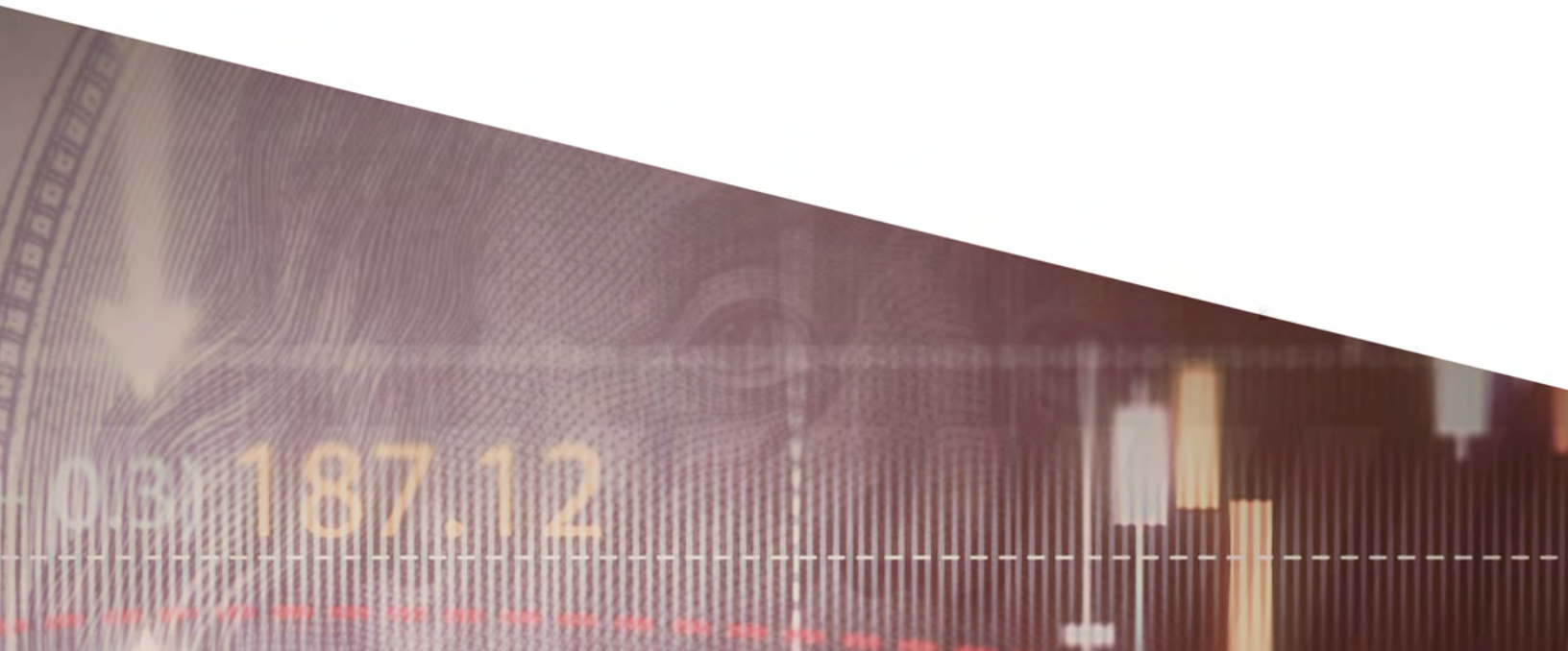
## The Industry Analysts' View of Bot Management

Increasingly, the major industry analyst firms are realizing that bot management was a blind spot in the cybersecurity landscape. They're recommending that for comprehensive web application security, addressing bad bots is a key component. The days of only considering DDoS and web application firewall (WAF) solutions are over. Then in Q3 2018, Forrester released its first evaluation of bot management vendors.

## The Evolution of Bad Bots is an Arms Race

Bad bots are evolving and are more sophisticated than ever. Increasingly they're mimicking real human workflows across web applications to "behave" like real users. Bots are obfuscating their activity by reverse engineering detection systems. Advanced attackers now show definitive behavior that they know about the technology they're trying to defeat, and they're continuously learning how to adapt their tactics. For example, there are 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.

> *"The bot arms race is very real; bot defenders and bot operators are playing a continual game of cat and mouse."*



# What Bad Bots Do

## Price Scraping

**How it hurts the business**

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

**Signs you have a problem**

Declining conversion rates

Your SEO rankings drop

Unexplained website slowdowns and downtime, usually caused by aggressive scrapers

**Industries Targeted**

All businesses that show prices:

- Ecommerce
- Gambling
- Airlines
- Travel

## Content Scraping

**How it hurts the business**

Proprietary content is your business. When others steal your content they are a parasite on your efforts

Duplicate content damages your SEO rankings

**Signs you have a problem**

Your content appears on other sites

Unexplained website slowdowns and downtime, usually caused by aggressive scrapers

**Industries Targeted**

Similar to price scraping, but in addition:

- Job boards
- Classifieds
- Marketplace
- Digital Publishing
- Real Estate

## Account Takeover
(a.k.a Credential Stuffing / Cracking)

**How it hurts the business**

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

**Signs you have a problem**

Increase in failed logins

Increase in customer account lockouts and customer service tickets

Increase in fraud (lost loyalty points, stolen credit cards, unauthorized purchases)

Increase in chargebacks

**Industries Targeted**

Any business with a login page requiring username and password

## Account Creation
(a.k.a Account Aggregation)

**How it hurts the business**

Free accouns used to spam messages or amplify propaganda

Exploit any new account promotion credits (money, points, free plays)

**Signs you have a problem**

Abnormal increases in new account creation

Increased comment spam

Drop in conversion rates of new accounts to paying customers

**Industries Targeted**

Messaging platforms:

- Social media
- Dating sites
- Communities

Promotion abuse

- Gambling

## Credit Card Fraud
(a.k.a. Carding, Card Cracking)

**How it hurts the business**

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 chargebacks

**Signs you have a problem**

Rise in credit card fraud

Increase in customer support calls

Increased chargebacks processed

**Industries Targeted**

Any site with a payment processor

## Denial of Service

**How it hurts the business**

Slows the website performance causing brownouts or downtime

Lost revenue from unavailability of website

Damaged customer reputation

**Signs you have a problem**

Abnormal and unexplained spikes in traffic on particular resources (login, signup, product pages, etc.)

Increase in customer service complaints

**Industries Targeted**

All industries

## Gift Card Balance Checking

**How it hurts the business**

Steal money from gift card accounts that contain a balance

Poor customer reputation and loss of future sales

**Signs you have a problem**

Spike in requests to gift card balance

Increase in customer service calls about lost balances

**Industries Targeted**

Ecommerce

## Denial of Inventory

**How it hurts the business**

Bots hold items in shopping carts, preventing access by valid customers

Damaged customer reputation because unscrupulous middlemen hold all inventory until resold elsewhere

**Signs you have a problem**

Increase in abandoned items held in shopping carts

Decrease in conversion rate

Increase in customer service calls about lack of availability of inventory

**Industries Targeted**

Scarce or time-sensitive items

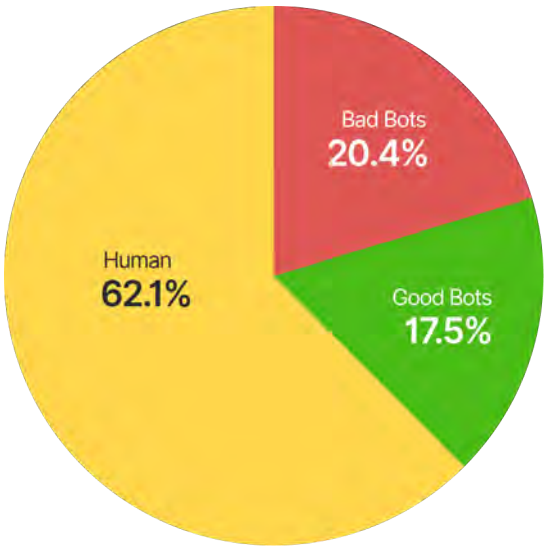
- Airlines
- Tickets

# Executive Summary of Findings

## Bad Bot Traffic Slightly Less

In 2018, 37.9% of all internet traffic wasn't human, and there were year-over-year decreases in both bad bot (-6.4%) and good bot (-14.4%) traffic. Human traffic increased by 7.5% to 62.1%

Bad Bot vs. Good Bot vs. Human Traffic 2018



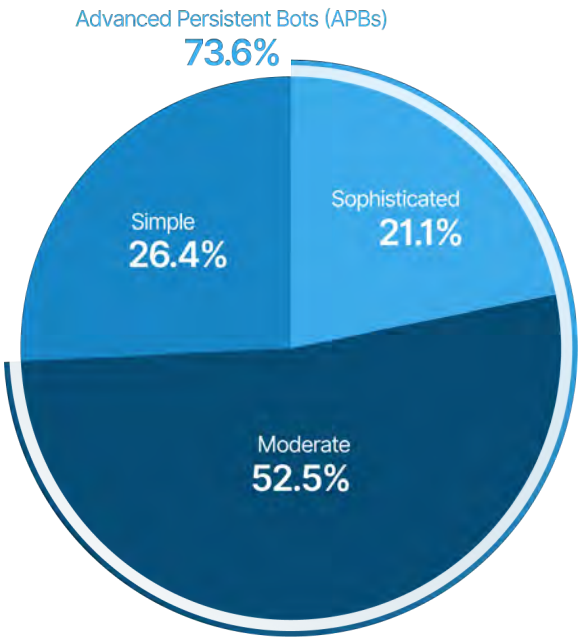

| | |
|---|---|
| Bad bots among all website traffic in 2018 | 20.4% |
| Change in bad bot traffic from previous year | -6.4% |
| Good bot traffic percentage in 2018 | 17.5% |
| Change in good bot traffic from previous year | -14.4% |
| Human website traffic percentage in 2018 | 62.1% |
| Change in human traffic from previous year | +7.5% |

## Bad Bot Sophistication Levels Remain Consistent

Advanced persistent bots (APBs) continue to plague websites. APBs cycle through random IP addresses, enter through anonymous proxies, change their identities, and mimic human behavior.

| | |
|---|---|
| Advanced Persistent Bots (Moderate + Sophisticated bad bot percentage) | 73.6% |
| Sophisticated Bots | 21.1% |
| Moderate bad bots | 52.5% |

Bad Bot Sophistication Levels 2018



## The Bot Problem Affects Every Industry

Some bad bot problems run across all industries while others are industry-specific. Websites with login screens are hit by bot-driven account takeover attacks two to three times per month. Content and price scraping is rampant and is undertaken by bots. Meanwhile, nefarious competitors use bots to undercut prices on ecommerce sites, hoard seats on airline flights, and scalp the best concert tickets.

### Top 5 Industries Bad Bot Traffic %

| | | |
|---|---|---|
| 1 | Financial | 42.2% |
| 2 | Ticketing | 39.3% |
| 3 | Education | 37.9% |
| 4 | IT & Services | 34.4% |
| 5 | Marketing & Advertising | 33.3% |

### Top 5 Industries Sophisticated Bad Bot Traffic %

| | | |
|---|---|---|
| 1 | Ticketing | 27.7% |
| 2 | Healthcare | 24.1% |
| 3 | Directories & Classifieds | 22.3% |
| 4 | Ecommerce | 21.4% |
| 5 | Marketplace | 21.0% |

## Half of Bad Bots Claim to Be Google Chrome

Bad bots continue to follow the trends in browser popularity, impersonating the Chrome browser 49.9% of the time. The use of data centers reduced in 2018 with 73.6% of bad bot traffic emanating from them—down from 82.7% in 2017.

| | |
|---|---|
| Bad bots report as either Chrome, Firefox, Internet Explorer, Safari | 78.1% |
| Bad bots hiding in data centers | 73.6% |
| Bad bots using Amazon ISP | 18.0% |

## Bad Bots Are All Over the World

With most bad bot traffic originating from data centers, the United States remains the “bad bot superpower” with over half of bad bot traffic coming from the country. A third of companies block Russia—the most blocked country for the second year running. Amazon was the source of the most global bad bot traffic at 18.0%.

### Top 5 Bad Bot Traffic by Country

| | | |
|---|---|---|
| 1 | United States | 53.4% |
| 2 | Netherlands | 5.7% |
| 3 | China | 3.9% |
| 4 | Germany | 3.9% |
| 5 | Canada | 3.2% |

### Top 5 Most Blocked Country

| | | |
|---|---|---|
| 1 | Russia | 32.6% |
| 2 | Ukraine | 15.6% |
| 3 | India | 15.2% |
| 4 | China | 11.2% |
| 5 | United States | 6.6% |

# The Bad Bot Landscape

## What is a bad bot?

Bad bots scrape data from sites without permission in order to reuse it (e.g., pricing, inventory levels) and gain a competitive edge. The truly nefarious ones undertake criminal activities, such as fraud and outright theft.

The Open Web Application Security Project (OWASP) provides a list of the different bad bot types in its Automated Threat Handbook. [4]

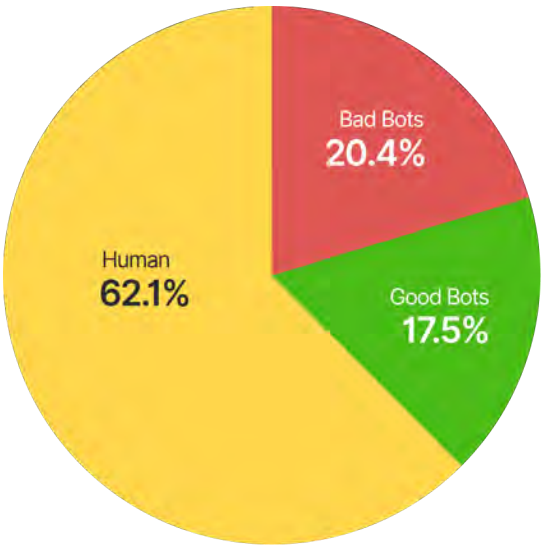
## How Do Good and Bad Bots Differ?

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. Being able to intelligently separate traffic generated by legitimate human users, good bots, and bad bots is essential for making informed business decisions.

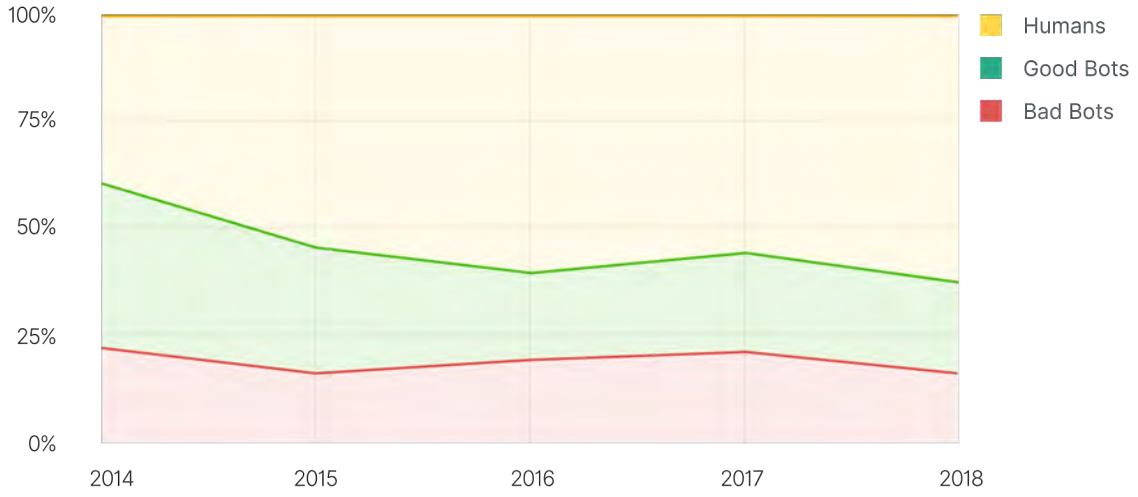
Bad Bot vs. Good Bot. vs Human Traffic 2018




In 2018, bad bots accounted for 20.4% of all website traffic—a 6.35% decrease over the prior year. Good bots decreased by 14.4%, accounting for 17.5% of all traffic. This past year the proportion of human traffic increased by 7.5%, totalling 62.1% of all internet traffic.

[4] www.owasp.org/images/3/33/Automated-threat-handbook.pdf

Bad Bot vs. Good Bot vs. Human Traffic 2014 - 2018




Bad Bot vs. Good Bot vs. Human Traffic 2014 - 2018

| | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| Bad Bots | 22.8% | 18.6% | 19.9% | 21.8% | 20.4% |
| Good Bots | 36.3% | 27.0% | 18.8% | 20.4% | 17.5% |
| Humans | 40.9% | 54.4% | 61.3% | 57.8% | 62.1% |

The bad bot traffic percentage has decreased slightly for the first time since 2015, but still accounts for 1 in 5 web requests.

The good news is that the number of human users is up in comparison with bots for the first time since 2016. But it's still surprising to see that human traffic comprises only 62% of all internet traffic. When the goal is to attract real humans to your website, these numbers show that the bot problem is still significant.

## Bad Bot Sophistication Levels

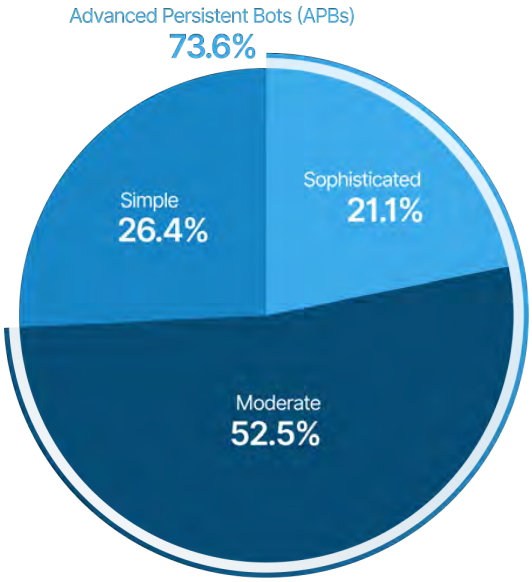
Distil Networks created the following industry standard system that classifies the sophistication level of the following four bad bot types:

- **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.

Bad Bot Sophistication Levels 2018




- **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 persistency on target sites.

*For the second year in a row, the sophistication levels are very similar.*

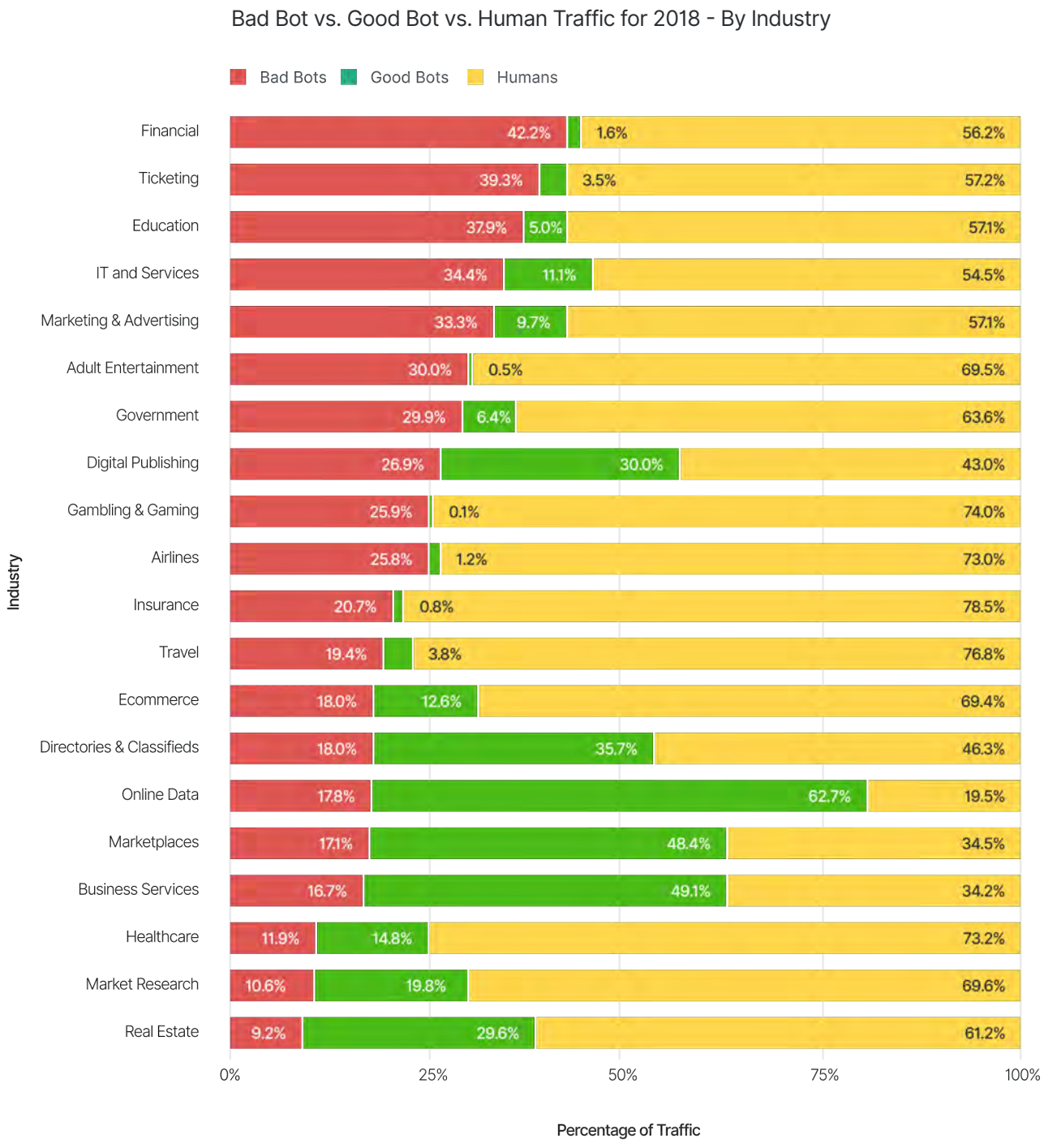
Simple bots, which are easiest to detect, accounted for 26.4% of bad bot traffic. Meanwhile, the majority of non-human traffic (52.5%) came from those classified as moderate. And sophisticated bad bots, the most difficult to detect, comprised of 21.1% of automated traffic last year.

Advanced persistent bots (APBs) accounted for 73.6% of all 2018 bad bot traffic—almost matching the prior year. Because they can cycle through IP addresses and switch user agents, simple IP blacklisting is wholly ineffective.

Known as "low and slow," APBs carry out significant assaults 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

By examining traffic from various industries, a deeper insight into the bot problem is possible. As more organizations add bot management to their security profile, a larger data set is gathered across more industries. For the 2018 Bad Bot Report, data was collected from 11 industries. For this report the number of industries expanded to 20.




Note: Minimum required to include an industry segment = 100 million requests

### Financial Services

Financial Services companies have the highest percentage of bad bots with 42.2%. Such companies typically suffer from bad bots attempting to access user accounts.

### Ticketing

One of the first industries targeted by bad bots, has the second highest percentage with 39.3%. Scalping bots, seat inventory checkers, and credential stuffing bots that access user accounts are most prevalent on these sites.

### Education

A new industry sector included in this study, had 37.9% bad bot traffic. Bots are deployed by malicious operators looking for research papers, class availability, and to access user accounts.

### Government

Government with 29.9% of bad bots, is interested in protecting business registration listings from scraping bots, and in stopping election bots from interfering with voter registration accounts.

### Gambling and Gaming

Gambling and Gaming companies, with 25.9% of bad bot traffic, suffer from aggregators relentlessly scraping for ever-changing betting lines. Account takeovers are also a major problem because each account contains money or loyalty points that, once compromised, can easily be transferred to another user and emptied.

### Airlines

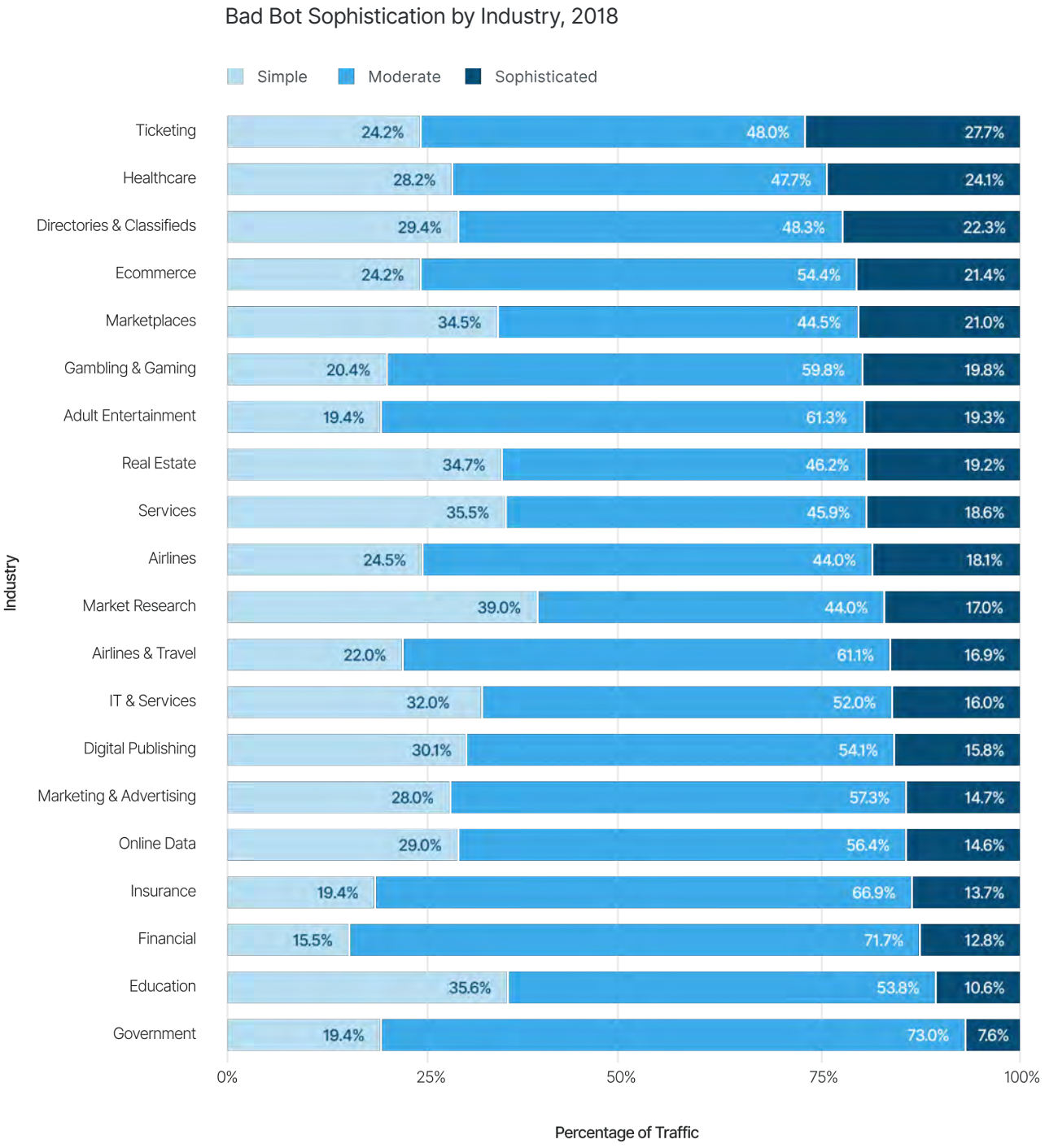
Airlines have a challenging problem with 25.9% of their traffic comprising bad bots. Prices are scraped not only by direct competitors, but also by third-party players in the expansive travel ecosystem. Unauthorized online travel agencies (OTAs), competitors, price aggregators, and metasearch sites use 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. In addition, airlines suffer from account takeover issues as bad bot operators attempt to get into user accounts and empty them of accumulated air mile balances.

### Ecommerce

Ecommerce companies see a wide range of bad bot attacks. These include price scraping, content scraping, account takeovers, credit card fraud, and gift card abuse. Having one of the largest datasets, ecommerce has 18.0% of the bad bot traffic.

## Bad Bots Sophistication by Industry

Comparing bad bot sophistication levels by industry reveals a very different picture. Ticketing, healthcare, directories & classifieds, and ecommerce see the highest proportion of sophisticated bots. It's important to understand that the volume of bots doesn't necessarily equate with sophistication. For example, a sophisticated bot may make fewer requests to achieve its goal.

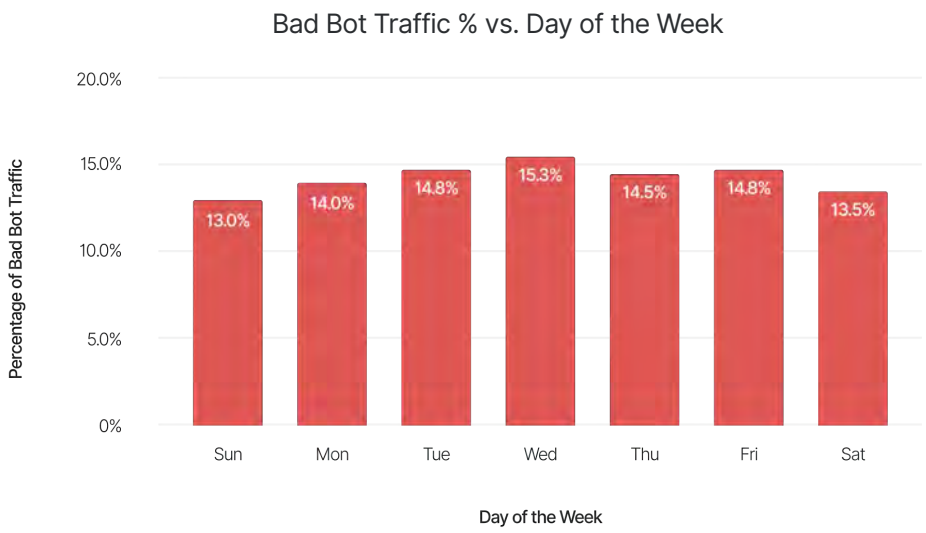


*"Bad bots continuously target all of these industries daily, with defenses requiring constant optimization. Every industry is attacked to check the viability of stolen credentials. Some are hit by sophisticated bots that repeatedly perform a specific task, such as checking credit card numbers. Another may be scraped for pricing content, while a third may be victimized by bad bots checking gift card balances.*

*Every bot problem is unique; factors to consider include the nature of the business, its website content, and the goal of the adversary. The bad bot problem affects every industry. But each company has a unique bad bot problem."*

## Bad Bot Traffic by Day of the Week

Wednesday was the most popular day for bad bot traffic in 2018. The consistency of such traffic on each weekday confirms the relentless nature of bots. The weekend is the lowest two days for bot traffic, which suggests that bot operators use bad bots as part of their day job.



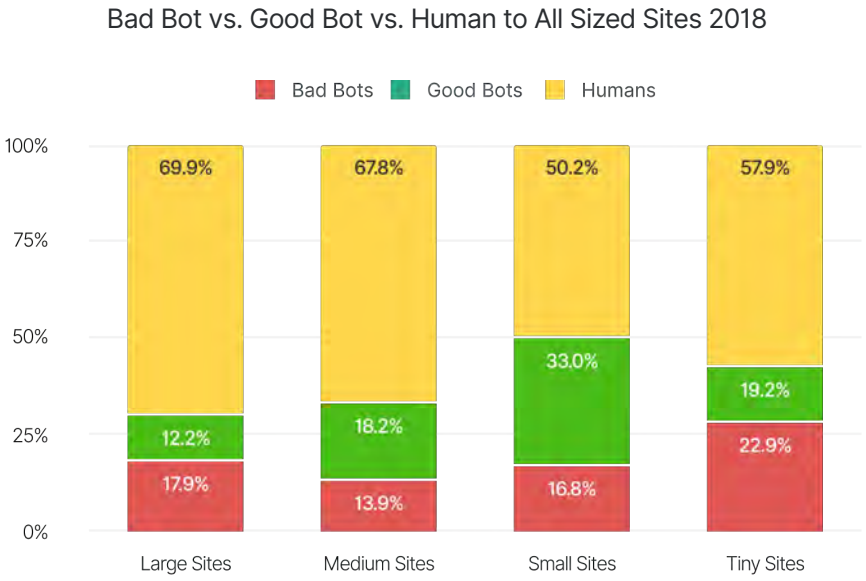

## Highest Bad Bot Traffic Day of 2018

The day with the most bad bot traffic in 2018 was March 27—a Tuesday.

## Bad Bots Traffic by Website Size 2018

Distil defines website size according to its Alexa index,[5] whereby sites are ranked by the amount of traffic received. An Alexa score of 1 means it's the most popular internet site—as of this writing that's Google.com. We used Alexa rankings to categorize sizes as follows:

- Large: Alexa 1 - 10,000
- Medium: Alexa 10,001 - 50,000
- Small: Alexa 50,001 - 150,000
- Tiny: Alexa 150,000+

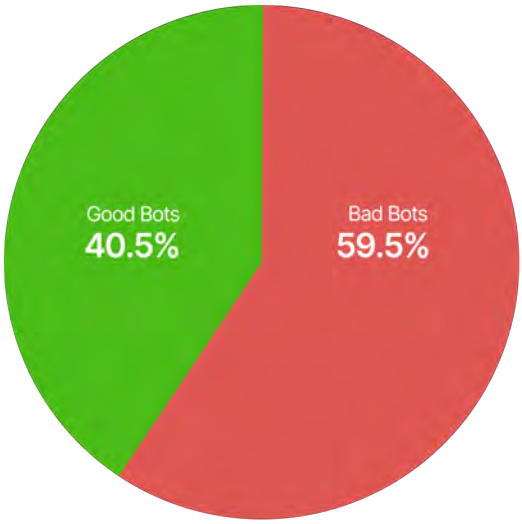



Bad bot volume is down for every website size. Tiny sites have the highest proportion of bad bot traffic at 22.9%, followed by large sites with 17.9%.

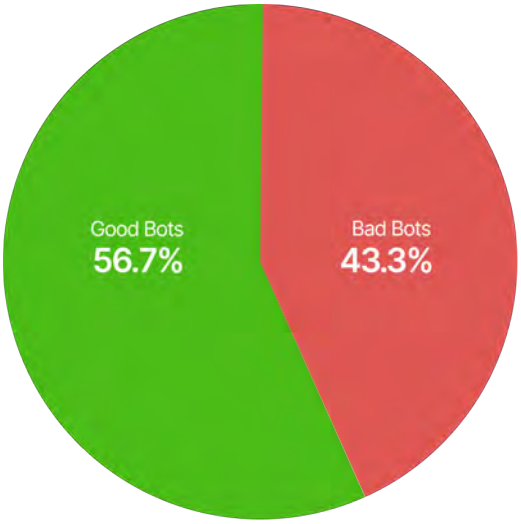
The following four charts show the bad to good bot traffic ratio for large, medium, small, and tiny sites. The highest ratio of bad bots (59.5%) to good bots (40.5%) is on large sites.

[5] Alexa.org

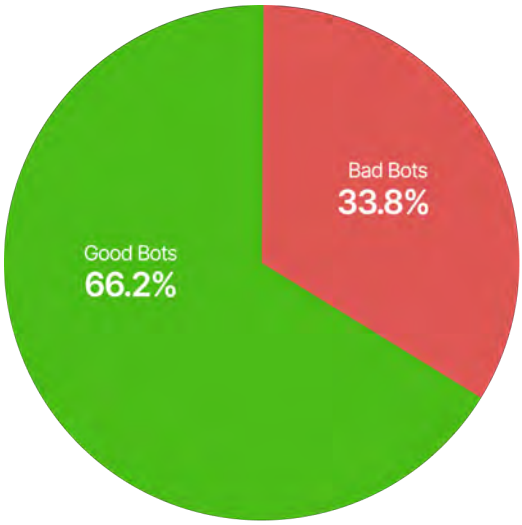
Bad Bot to Good Bot Ratio on Large Sites 2018



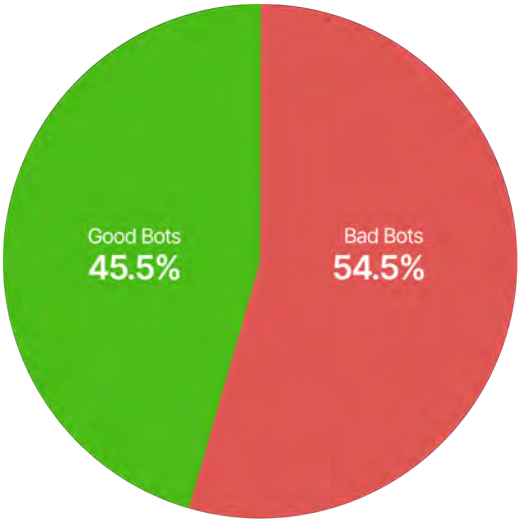

Bad Bot to Good Bot Ratio on Medium Sites 2018




Bad Bot to Good Bot Ratio on Small Sites 2018




Bad Bot to Good Bot Ratio on Tiny Sites 2018

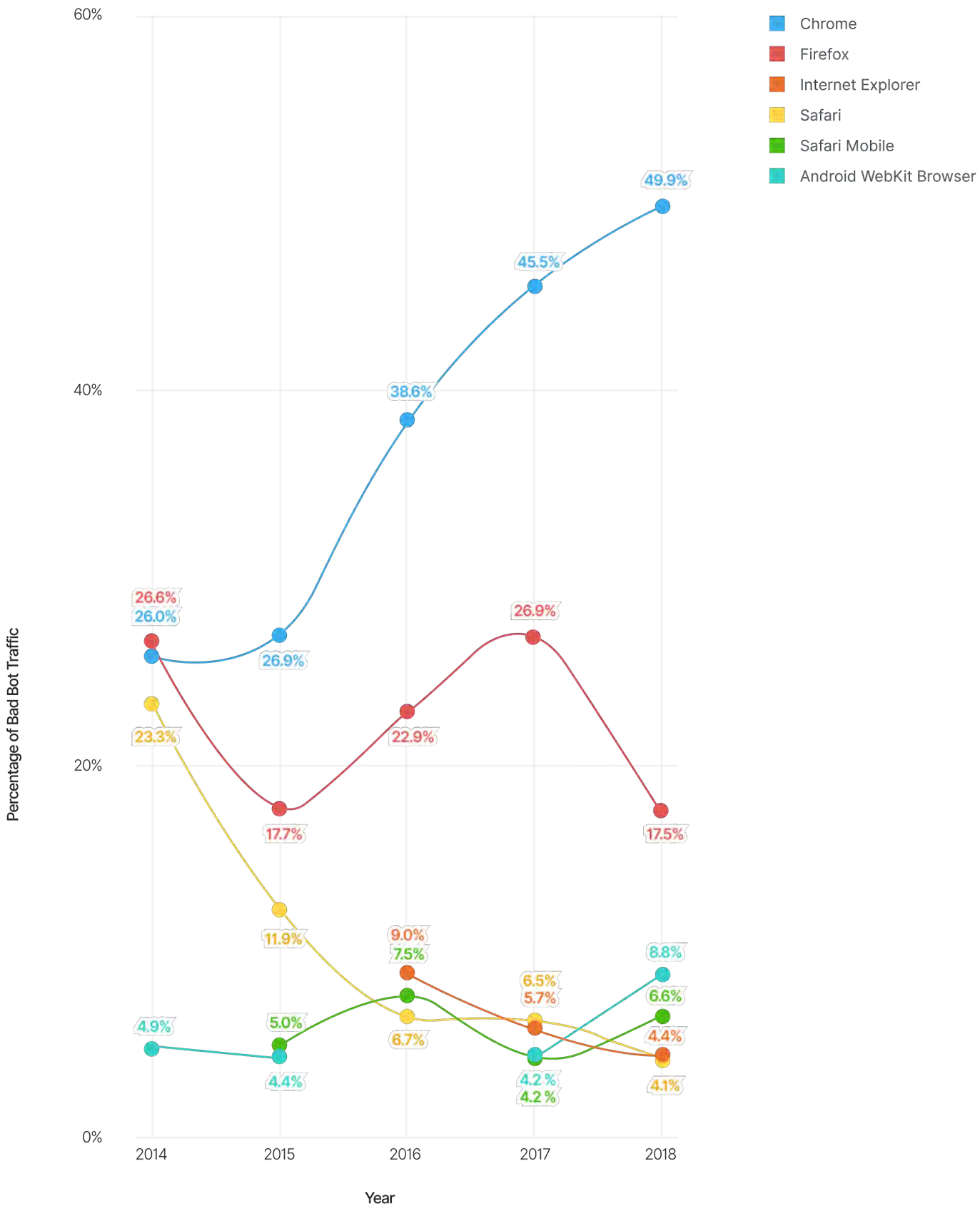



## Bad Bot Identity

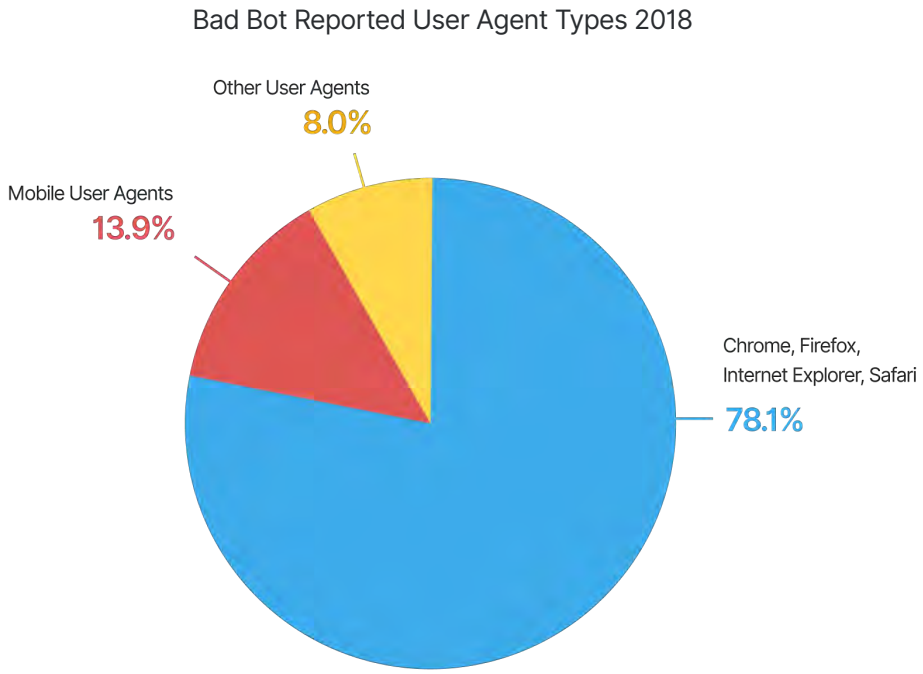
Bad bots must disguise their identity to avoid detection. They do so by reporting their user agent as a web browser or mobile device. While the majority of bad bots claim to be the most popular browsers, during 2018 bad bots claimed a total of 523 different identities (user agents).

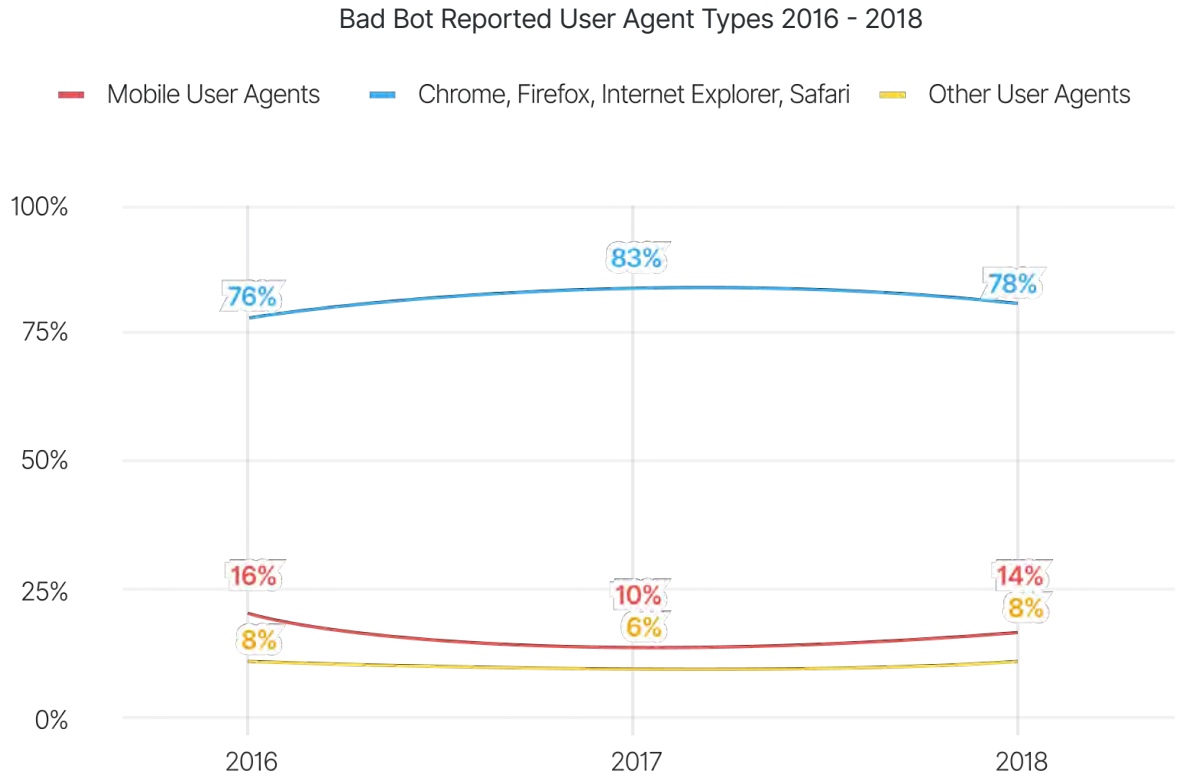
In 2018, Chrome continued to be the most popular fake identity used by bad bots, with almost half (49.9%) of them making this claim. Firefox dropped to 17.5% but is the second most popular claimed identity. Android WebKit Browser was claimed by 8.8% and is the only mobile browser in the top three.

Top Self-Reporting Browser by Bad Bots 2014 - 2018



The majority of bad bots (78.1%) self-reporting as either Chrome, Firefox, Safari, or Internet Explorer was slightly lower than the 83.2% of the previous year. Mobile browsers, such as Safari Mobile, Android, and Opera increased to 13.9% from 10.4% last year. The remaining 8% reported themselves as other user agents, such as Googlebot and Bingbot.



## The Bad Bots We Can't Forget

By seeing which user agent identity they claim, examining the age of bad bots shows that a small amount are using browsers that were released 20 years ago. For old browsers, the top ten are in the same order as last year. Released in 1999, Internet Explorer 5 was again the oldest. Internet Explorer 7 is used by 0.823% of bad bots.

Clearly, the easiest way to prevent bad bots from hitting your website is to block out-of-date user agents from gaining access.

## The 10 Oldest Self-Reported Browsers by Bad Bots 2018

| Year | Browser | Bad Bot Market Share % |
|---|---|---|
| 1999 | Internet Explorer 5 | 0.044% |
| 2000 | Internet Explorer 5.5 | 0.009% |
| 2001 | Internet Explorer 6 | 0.699% |
| 2002 | Netscape 7 | 0.051% |
| 2004 | Firefox 1 | 0.111% |
| 2005 | Netscape 8 | 0.002% |
| 2006 | Internet Explorer 7 | 0.823% |
| 2006 | Firefox 2 | 0.135% |
| 2007 | Netscape 9 | 0.002% |
| 2008 | Firefox 3 | 0.116% |

### Why Use Out-of-Date Browsers?

Perhaps some bad bots were written many years ago and remain on the prowl. Some may have targeted systems that only accept specific browser versions. Others may be out-of-control programs, bouncing around the internet in endless loops, still causing collateral damage.

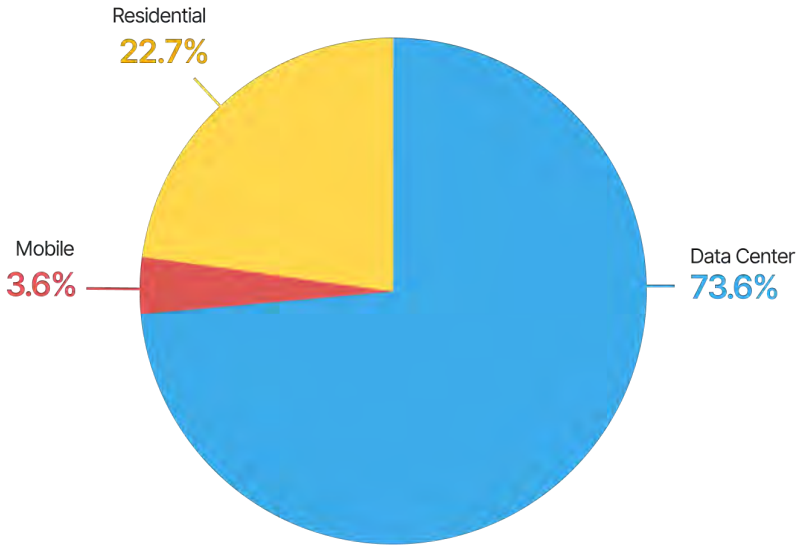
## Bad Bots Weaponize Data Centers

The weaponization of the data center continues, but was slightly less than the previous year. Almost three-quarters (73.6%) of bad bot traffic came from data centers in 2018, compared with 82.7% in 2017. The continued global availability of low-cost cloud computing is what accounts for this dominance of data center use.

Bad bot traffic from mobile ISPs increased - from 2.5% the year prior to 3.6% in 2018.

Residential bad bot traffic also increased from 14.8% to 22.7% in 2018.

Bad Bot Traffic by ISP Type 2018




## Bad Bots Abuse ISPs Globally

Bad bots were launched from 1,935 ISPs during 2018.

Amazon is the leading ISP for originating bad bot traffic. In 2018, 18.0% of bad bot traffic originated from it compared to 10.6% the previous year.

Last year's number one, OVH Hosting, dropped to fourth place with 3.1% bad bot traffic in 2018 compared with 11.6% the prior year.

Digital Ocean and Comcast Cable were the second and third largest sources of bad bot traffic.

## Top 10 Bad Bot Originating ISPs 2018

| Rank | ISP | % of Traffic |
|---|---|---|
| 1 | Amazon | 18.0% |
| 2 | Digital Ocean | 3.7% |
| 3 | Comcast Cable | 3.7% |
| 4 | OVH Hosting | 3.1% |
| 5 | Google | 2.2% |
| 6 | Spectrum | 2.1% |
| 7 | DataWeb Global Group B.V. | 1.9% |
| 8 | Microsoft Corporation | 1.8% |
| 9 | Cogent Communications | 1.5% |
| 10 | PT Telkom Indonesia | 1.1% |

## Top 10 Mobile ISPs

| Rank | ISP | % of Traffic |
|---|---|---|
| 1 | T-Mobile USA | 0.5% |
| 2 | Orange Espana | 0.5% |
| 3 | AT&T Wireless | 0.5% |
| 4 | China Telecom Guangdong | 0.5% |
| 5 | Telfonica de Espana | 0.5% |
| 6 | Virgin Media | 0.3% |
| 7 | Verizon Wireless | 0.3% |
| 8 | KPN | 0.3% |
| 9 | Orange | 0.2% |
| 10 | China Telecom Zhejiang | 0.2% |

## Mobile ISPs: Available if Needed

Data center traffic comprises the majority of bad bot traffic. But mobile ISPs also play an important role when bot operators find their data center traffic is blocked. Mobile ISP bad bot traffic is still a small percentage and is remaining at consistent levels compared with 2017.

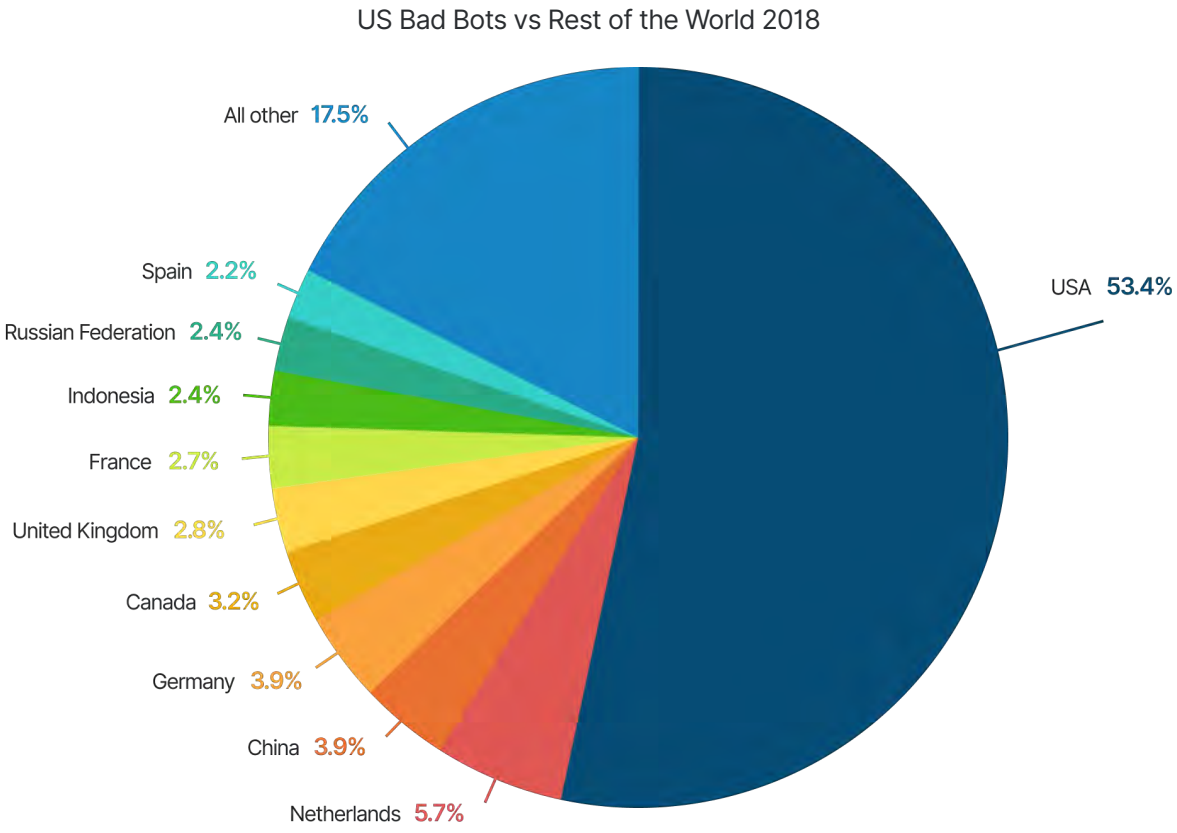
## USA: Where Half the World's Bad Bots Originate

For the fifth year running, the United States topped the list of bad bot originating countries. It remains the only bad bot superpower, from which more than half (53.4%) of all bad bot traffic originates.

The Netherlands has moved up to second place with 5.7% of all bad bot traffic—up from 3.1% the prior year.

China has dropped from second to third place and is responsible for 3.9% of bad bot traffic.

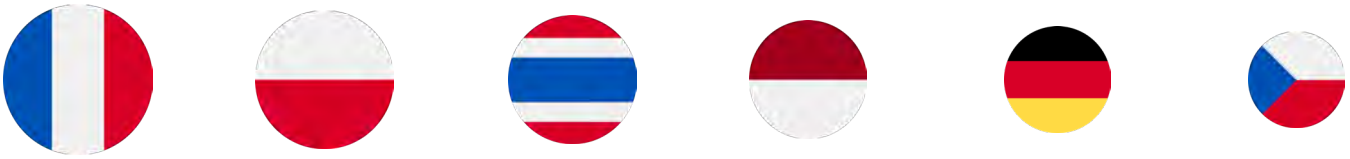
France has dropped from 9.9% the previous year to 2.7% in 2018.



## Russia: The Most Blocked Country

Russia is the most blocked country by Distil Networks customers for the second year running.

1 Russia | 2 Ukraine | 3 India | 4 China | 5 USA | 6 Brazil



7 France | 8 Poland | 9 Thailand | 10 Indonesia | 11 Germany | 12 Czech Republic

**Why Block Countries?**

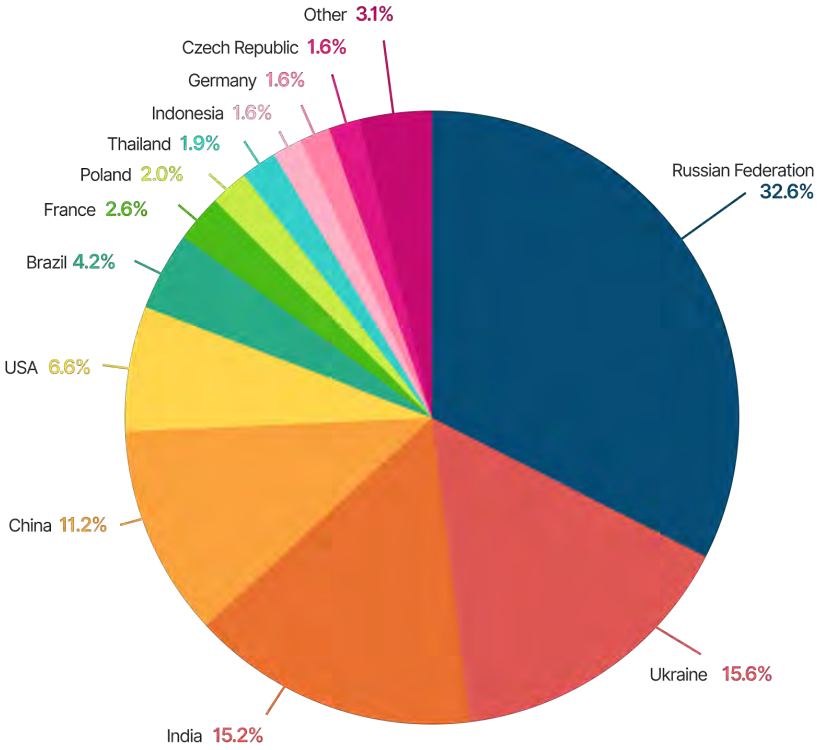
Many companies use geofencing blacklists to choke off large swaths of unwanted traffic. In some cases, it simply doesn't make sense that foreign visitors would use a given site, so blocking chunks of foreign IP addresses is good hygiene. In other situations, customers have suffered attacks from countries that haven't traditionally generated good traffic, so have taken sensible protection measures.

Because of its notorious status, a third (32.6%) of all blocking requests were preventing access from Russia.

Russia and Ukraine combined accounted for 48.2% of country-specific block requests.

For the second year running, the United States is on the most-blocked list, accounting for 6.6% of country-specific block requests.

India is now the third most-blocked country at 15.2%. This is a significant increase from the prior year when it was the 10th most blocked country (at 2.1%).



# Distil Research Lab

Additional research lab reports | www.distilnetworks.com/research-lab

Bad Bot Report archive | www.distilnetworks.com/bad-bot-report-archive

# Threat Research


### Mobile Bots: The Next Evolution of Bad Bots

***Key Finding***
*5.8% of mobile devices on cellular networks are used in bad bot attacks.*


### The Anatomy of Account Takeover Attacks

***Key Finding***
*Average of 2-3 account takeover attacks per month.*

# Industry Research


### How Bots Affect Airlines

***Key Finding***
*51 airlines with bad bot traffic higher than 50%.*


### How Bots Affect Ticketing

***Key Finding***
*Bad bot traffic is 39.9% across 180 ticketing domains.*

# Recommendations

Bots are on your website every day, and attack characteristics become more advanced and very 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.

## Recommendations for Detecting Bad Bot Activity

1. **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 step 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<br>End of Life<br>More than 3 years | CAPTCHA<br>End of Life<br>More than 2 years |
|---|---|---|
| Firefox version | < 38 | < 45 |
| Chrome version | < 41 | < 49 |
| Internet Explorer version | < 10 | 10 |
| Safari version | < 9 | 9 |

2. **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.

   Block these data centers:

   Digital Ocean | GigeNET | OVH Hosting | Choopa, LLC

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. Evaluate a Bot Mitigation 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 using 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 Distil Networks

Distil Networks, the global leader in bot mitigation, protects websites, mobile apps, and APIs from automated threats. Fraudsters, hackers, and competitors use bots to commit online fraud, break into customer accounts, and gain an unfair competitive advantage.

As the sheer volume, sophistication, and business damage of these attacks grow, bots put a costly strain on IT staff and resources. Only Distil's unique, more holistic approach provides the vigilant service, superior technology, and industry expertise needed for full visibility and control over such abusive traffic.

The Distil team pioneered bot mitigation in 2011 and has been leading the way ever since. With Distil, there is finally a defense against automated attacks that is as adaptable and vigilant as the threat itself.

For more information about Distil, visit https://www.distilnetworks.com/block-bot-detection/ or follow @distil on Twitter.

**Blue Cube**
**Intelligent Protection**



***Blue Cube Security is one of the UK's largest independent Information and Cyber Security solution providers. Leading with a consultative approach, Blue Cube Security has been providing expertise and agile services to its customers for over 19 years, operating nationally from a UK head office.***
***For more information, please visit www.BlueCubeSecurity.com***