imperva

IMPERVA REPORT

How Bots Affect Ticketing

Executive Summary of Findings

Bots by the numbers:

Bad bot traffic perentage - All industries	21.8%
Bad bot traffic percentage - Ticketing	39.9%
Highest bot traffic percentage on a ticketing domain	99.96%
Number of ticketing domains with greater than 40% bad bot traffic	32

Five Groups Attack Ticketing With Bots

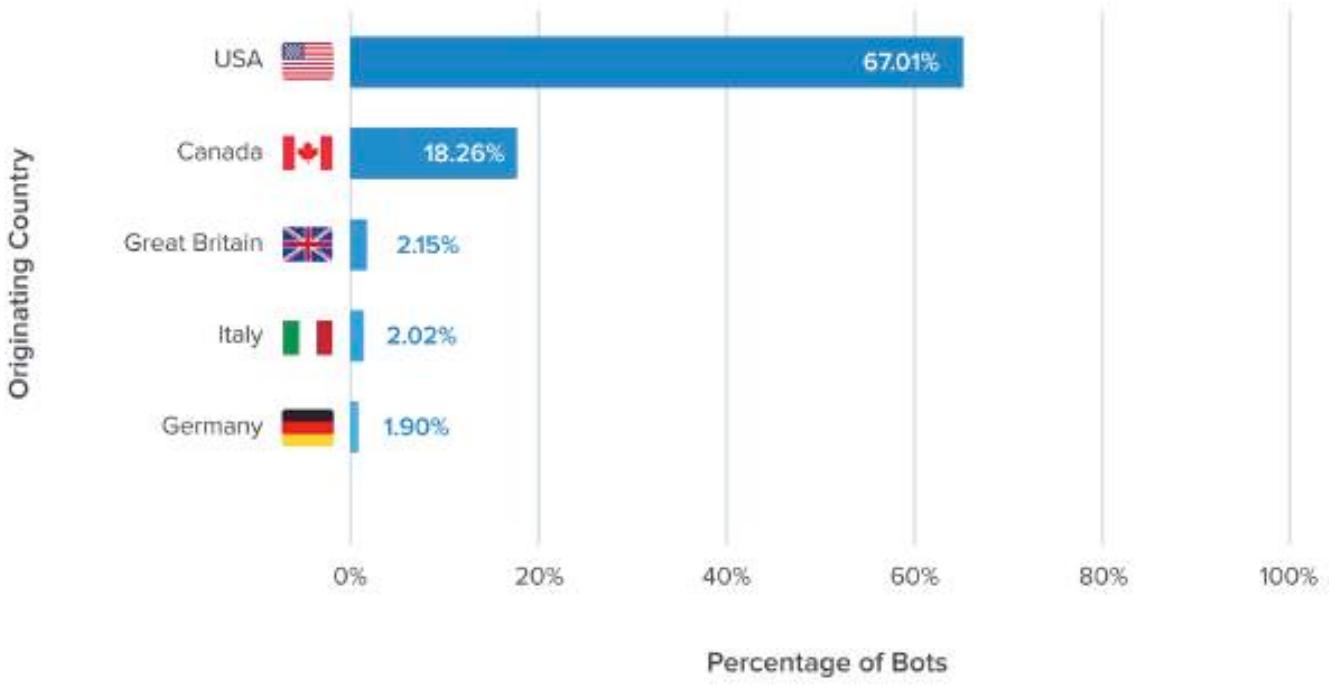
Who Launches Bots	Bot Objectives
Brokers Individual Scalpers	Scrape ticket details Instantly purchasing any available tickets to re-sell (Scalping) Continuously checking seat map inventory for newly released seats
Hospitality Agencies Corporations	Scrape ticket details Instantly purchasing best available tickets to re-sell Continuously checking seat map inventory for premium seats
Criminals	Account takeover to access fan accounts to steal tickets or transfer to another account Fraud - Credit card and loyalty fraud (Sports teams season ticket holders)

Bot Sophistication on Ticketing Rises

Bot Sophistication	Ticketing Domains 2017[1]	Ticketing Domains 2018
Sophisticated	19.10%	31.40%
Moderate	59.63%	46.60%
Simple	21.27%	21.90%

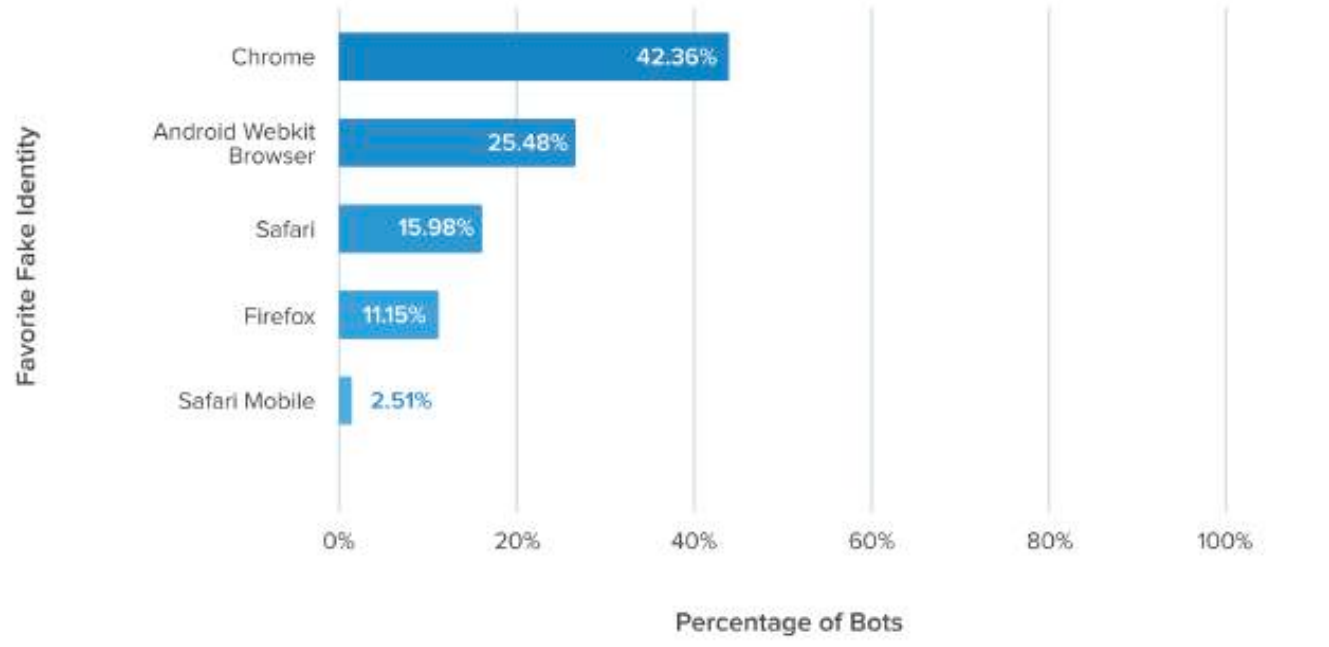
TOP 5

Ticketing Bot Traffic Originating Country



TOP 5

Ticketing Bots Favorite Fake Identity



Introduction to the Bad Bot Problem

Bad bots are a problem faced by every business with an online presence. Every website, mobile app, and the APIs that power them are attacked by bots around the clock. According to the annual Bad Bot Report, only 57.8 percent of web traffic comes from actual humans—the rest are bots. While some bots are welcomed by businesses, such as search engines, there are other nefarious bots that are dangerous to the success of organizations. These bad bots comprise 21.8 percent of all web traffic.

The Ticketing Bot Problem

The ticketing industry has a bad bot problem that is unique. In our previous bad bot study, we found that the percentage of web traffic on ticketing websites that can be attributed to bad bots was 22.97 percent, which is worse than the average for all industries. In this new study, bad bot traffic has risen to 39.9 percent. The increase is explained by a more robust dataset including a greater volume of traffic analyzed, and inclusion of data from a larger number of ticketing companies.

Interestingly, the proportion of human traffic on ticketing websites is similar to the average seen across all industries (3.2 percent). The major difference is within the composition of bot traffic. There are far more bad bots than good bots on ticketing domains. This lower proportion of good bots is explained in two ways.

First, good bot traffic is small compared to the sheer volume of human requests looking to buy tickets. Second, the scale of bad bot requests is massive because bad bots check for tickets around the clock. In comparison, good bot requests, like those from search engines, are small in volume and occur less frequently.

Historically, ticketing has led the way in the evolution of the bot problem. As the ticketing industry moved online, it was the first industry to suffer from nefarious bot operators who used automated attacks to hold and scalp tickets. Following customer complaints and pressure from artists, it was also the first industry to adopt legislation intended to fight bad bots.

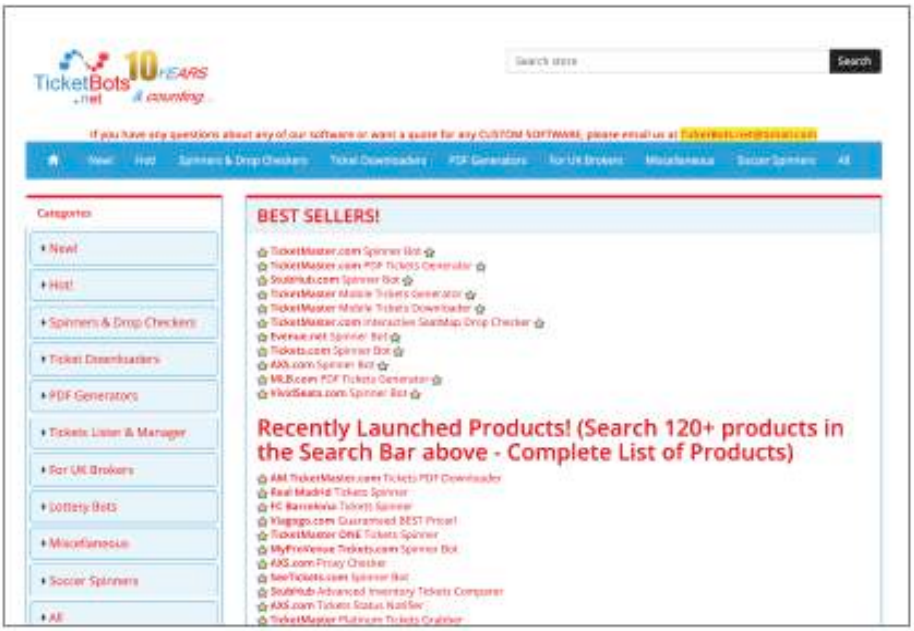
In the U.S., the 2016 Better Online Ticket Sales Act, commonly known as the BOTS Act, outlawed the resale of tickets purchased using bot technology and imposed fines for violations. The United Kingdom, Australia, and parts of Canada have also enacted similar legislation. While the adoption of legislation is a step in the right direction, many countries have yet to fully explain how enforcement of these new laws will be funded or policed.

An Industry Under Constant Attack

While bad bots cause frustration among fans who are unable to purchase tickets to performances by their favorite artists, ticketing platforms also suffer significant impacts. It is appropriate to look at the bad bot problem from the industry point of view.

To fully grasp the scale of the around-the-clock battle that ticketing companies fight every day, consider that there are e-commerce businesses such as ticketbots.net that sell malicious bots to anyone looking to take advantage of any ticketing platform. A quick scan of the ticketbots.net homepage reveals the multitude of bad bots that are available for purchase, the ticketing platforms they exploit, even the specific sports teams they target. The website even offers to provide "quotes for any CUSTOM SOFTWARE." (See immediately below the ticketbots.net logo.)

This is the environment that primary ticket platforms work in every day. No matter what preventative measures ticketing platforms adopt to provide fair access to tickets, there are economically motivated adversaries actively looking to escalate the arms race.



Bots in the Ticketing Ecosystem

This report is the first industry-specific study into the round-the-clock damage caused by bots on ticketing websites, APIs, and mobile apps. Before delving into the statistical data, it is helpful to understand why bots are used, what types of bot operators are using them, and the business impact on ticketing companies.

SPECIFIC EVENT INFORMATION	SEAT MAP	CUSTOMER ACCOUNT PAGES
Including venue, pricing, date & time, and payment process	Showing availability of inventory	Accessed using credentials and stores purchased tickets, loyalty points, and personally identifiable information

Ticketing Web Property Structure

Ticketing websites and mobile apps are at the heart of the bot problem. They are the online home for all event information that is presented to customers who make purchase decisions, select seats at different pricing tiers, process payments, and select delivery methods for their purchased tickets.

For simplicity, ticketing websites can be thought of as having three distinct areas:

Regardless of the specific technical structure of the website, bots plague all ticketing platforms. In general, they are launched from five main groups of bot operators.

Bot Operators: Brokers

Brokers sell and distribute tickets to fans all over the world. Authorized brokers are given access to seats, sometimes in advance of general availability, based on negotiated commercial terms, or in exchange for associated fees. To understand the supply and demand for tickets to an event, they use bots to gain market intelligence on current seat prices, determine the current availability of tickets, and purchase available tickets to resell at a higher price. (Also known as scalping). Brokers scrape this data from ticketing platforms using automated scripts that run when programmed—otherwise known as scalper or spinner bots.

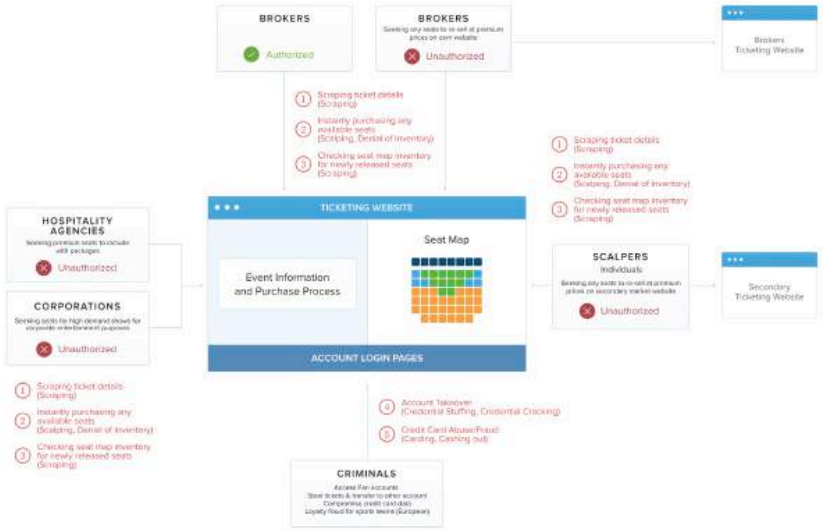
Unauthorized brokers also use bots to scrape the same ticket information, check inventory, and rapidly purchase tickets once they are available. The difference here is they do so with no agreement with the ticketing platform. Unauthorized brokers use automation to purchase tickets in volume and use arbitrage to resell them at premium prices on their own websites.

Unscrupulous brokers also use bad bots to create the secondary market for an event by holding (spinning) or purchasing all available seats on a ticketing platform which prevents real humans from being able to purchase tickets. Frustrated fans abandon the primary ticket platform,

search for tickets on broker sites, and pay the premium to get a seat.

Unauthorized brokers also use bots to scrape the same ticket information, check inventory and rapidly purchase tickets once they are available during an onsale. The difference here is they do so with no agreement with the ticketing platform. Unauthorized brokers seek to use automation to purchase tickets in volume and use arbitrage to resell them at premium prices on its own website. Unscrupulous brokers also use bad bots to create the secondary market for a show by holding (spinning) or purchasing all available seats on the ticketing platform preventing real human access. Frustrated fans abandon the primary ticket platform and search for tickets on broker sites and must pay the premium to gain a seat.

The Ticketing Ecosystem Affected by Bots



Bot Operators: Individual Scalpers

Individual scalpers, also known as touts, run a business using techniques that are similar to those that brokers use, but on a smaller scale. Scalpers deploy bots to hold or purchase seats made available at the start of an onsale, then resell or scalp the tickets on the secondary market. The difference between individual scalpers and brokers is that individuals don't use their own website to resell the tickets. Instead, they use any of the popular secondary-market ticketing platforms. Individual scalpers also deploy bots to continuously check inventory for any newly released tickets.

Bot Operators: Hospitality Agencies

Hospitality agencies are another outlet for tickets. Typically, the tickets are bundled together within packages of premium services including transportation, meals, and other VIP events. To create such premium packages, hospitality agencies need access to the best available seats. Bots are used to check inventory for premium seats and purchase any identified as available.

Bot Operators: Corporations

Surprisingly, some well-known corporations deploy bots against ticketing platforms to gain access to seats for high-demand events. Corporations use these tickets for corporate entertainment purposes such as perks for their clients or executives.

Bot Operators: Criminals

Criminals primarily launch bots on ticketing platforms in order to compromise customer accounts. They use bots to release brute-force credential stuffing and credential cracking attacks that steal stored tickets, credit card information, and personal information.

Credit card fraud like card cracking is also performed by bots. Access to customer accounts exposes the possibility of fraud from loyalty programs offered by some sports teams within their season ticket programs. This is most prevalent with season ticket holders in European soccer.

Account takeover shakes the confidence of fans so much that many will no longer use the ticketing platform where their account was compromised. Once a customer has been locked out of their account by a criminal changing their password, the ticketing company has a customer service problem to solve. The forensics to investigate what happened inside the account is time-consuming and costly. Also, there is the cost of reimbursement for theft or credit card fraud.

How Bots Affect Ticketing

Ticketing companies are in a constant war against bots. The barrage of bots cause continuous problems such as unauthorized scraping, seat spinning, scalping, inventory checking, fan account takeover, ticket theft, and fraud. Each of these problems alone is enough to have a significant impact on customer experience and, ultimately, the reputation of the ticketing platform. Collectively, these bot activities can add up to a significant headache for the business, especially the IT team. Left unaddressed, they lead to poor website performance and even downtime.

The Primary Problem is Denial of Inventory for Real Fans

When an onsale is launched and spinner bots are used by brokers, scalpers, hospitality agencies, and corporations to purchase tickets within milliseconds of them going on sale, real humans cannot successfully use the website or mobile app to purchase tickets. Frustrated fans often blame the ticketing platform. The most vocal of them turn to social media to make their frustrations known to artists who, in turn, apply pressure on ticketing companies to provide a better fan experience.

Seat Spinning: Creating the Secondary Market

The process of using bots to hold and purchase seats as soon as an onsale begins not only blocks real fans from gaining access to tickets, it also helps create the secondary ticket market. A frustrated fan who unsuccessfully attempts to buy a ticket on the primary market will quickly turn to secondary ticketing marketplaces or broker websites, only to face further frustration when they find considerably higher ticket prices. This further damages the reputation of the ticketing platform in the eyes of the fan. Adding insult to injury, the additional money spent by the fan goes into the pocket of the bot operator and not the primary ticketing platform.

Typically, the volume of scalping is highest on primary ticket markets. The number of scalpers found on secondary market websites is considerably lower because premiums are already added to the ticket pricing when they are posted on secondary markets, diminishing the opportunity for further arbitrage.

Checking Seat Map Inventory

Many events release their tickets in stages over a period of time. Bots are used by brokers, scalpers, hospitality agencies, and corporations that continue checking for new seats to become available. Premium seats for high-demand events are difficult for real fans to purchase because bot operators program their bots to locate and buy them the moment they become available.

This volume of inventory checking bots is significant and continuous. Ticketing platforms must spend money on additional infrastructure to make sure their website doesn't suffer from brownouts or downtime.

Account Takeover

Bots run credential cracking and credential stuffing attacks to identify pairs of usernames and passwords that unlock access to accounts.

Credential cracking attempts, where a bot is programmed to try common passwords with stolen email addresses (known as a dictionary attack)

are typically low and slow and occur consistently around the clock.

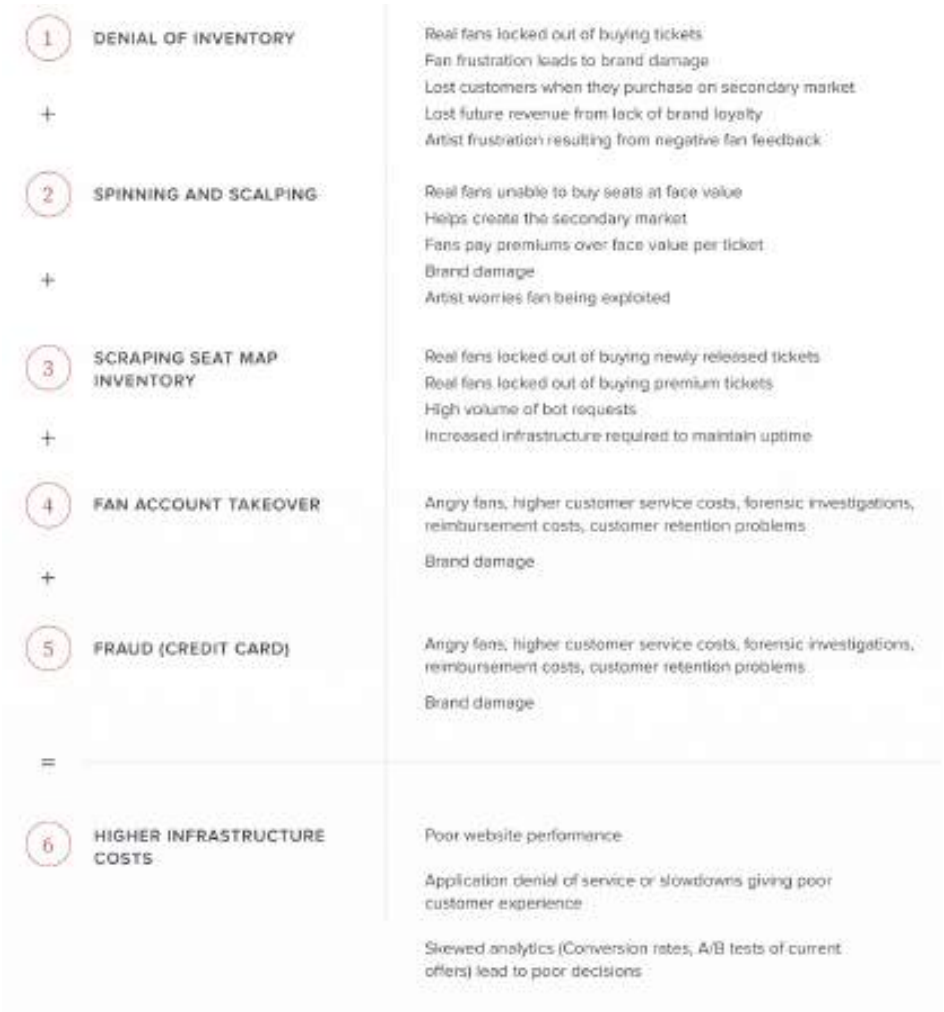
Credential stuffing attacks are when a criminal runs a list of stolen, paired credentials against sites around the world, hoping to gain access. They are volumetric in nature. These attacks are spikey and last for a short period. If they are large enough, credential stuffing attacks can cause website slowdowns or downtime due to the demand they place on the backend database during repeated authentication attempts. Because the vast majority of stolen credentials fail during a credential stuffing attack, it is sensible to conclude that any sudden spike of traffic to a login page, combined with a higher than normal failed login rate, is an indicator of account takeover attempts by bots.

An increase in complaints about the loss of loyalty points is another indicator of bot activity resulting from account takeover. In Europe, for example, we see especially high rates of loyalty point theft from season ticket holders of many soccer teams.

Accounts on secondary-market ticketing websites are targets of account takeover more often than accounts on primary platforms because they hold both tickets that are being sold and any currency or credits exchanged in the sale of tickets.

Fraud: A Cost of Doing Business?

Credit card fraud is a constant problem for any e-commerce business, and ticketing platforms are no different. Card-not-present transactions are necessary but lead to an increase in options for criminals attempting to commit fraud using stolen or incomplete credit card details. Bots are used to run carding and card cracking scams. Any increase in customer complaints about account lockouts or an increase in credit card fraud is a good indicator of the presence of malicious bots. Reducing the total volume of bot traffic on the website or mobile app typically lowers the amount of attempted automated fraud during transactions.



Methodology

This report is the first industry-specific study into the round-the-clock damage caused by bad bots on ticketing websites, APIs, and mobile apps. This report is based on an aggregate of data gathered from 180 domains and does not reveal data from any specific company.

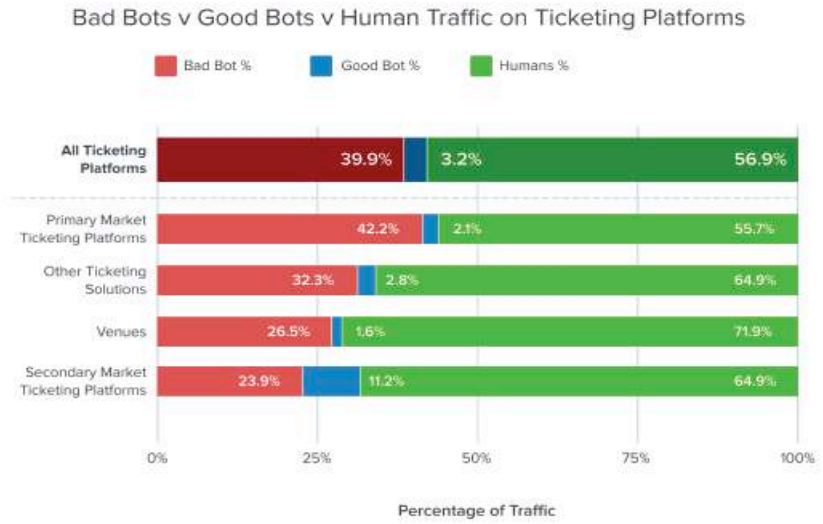
Number of Domains	180
Time Period	105 Days
Date of Data Gathering	Sep-Dec 2018
Number of Requests Analyzed	26.3 billion

The Bots on Ticketing Platforms

Across all 180 ticketing domains we studied, 39.9 percent of traffic came from bad bots. The primary-market ticketing platforms, where tickets

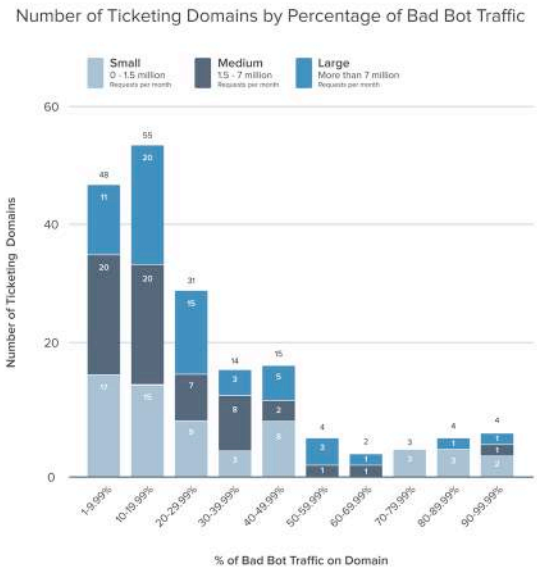
are first made available, suffered the most with 42.2 percent of traffic coming from bad bot traffic. They are inundated with automated attacks around-the-clock, particularly from scalper and inventory-checking bots.

The secondary-market ticketing platforms see considerably less bad bot traffic (23.9 percent) and see far less scalper bots. Instead, they have a significant problem with credential stuffing and credential cracking bots that try to takeover accounts. Venues saw 26.5 percent of their traffic coming from bad bots. All other ticketing solution websites that don't not fall into primary, secondary market, or venues, averaged 32.3 percent bad bot traffic.



How Bad is Bad?

The highest proportion of bot traffic we found in this study was on a secondary-market ticketing platform. A whopping 99.96 percent of its traffic came from bad bots; humans accounted for only 0.03 percent of its traffic. Thirty-two of the domains we studied suffered from over



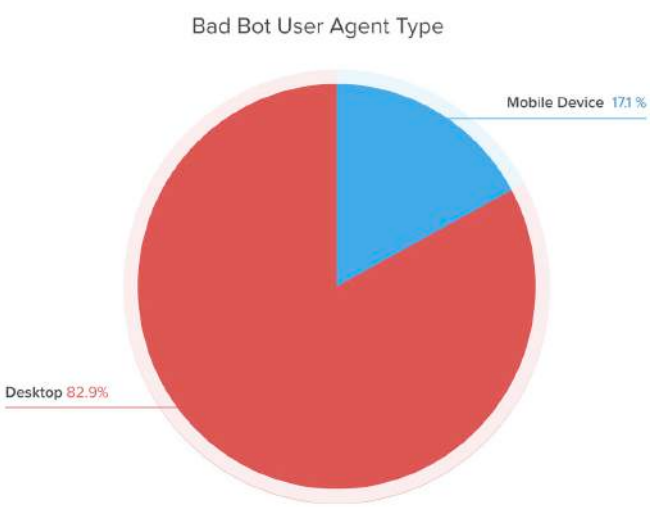
Ticketing Bot Sophistication Rises

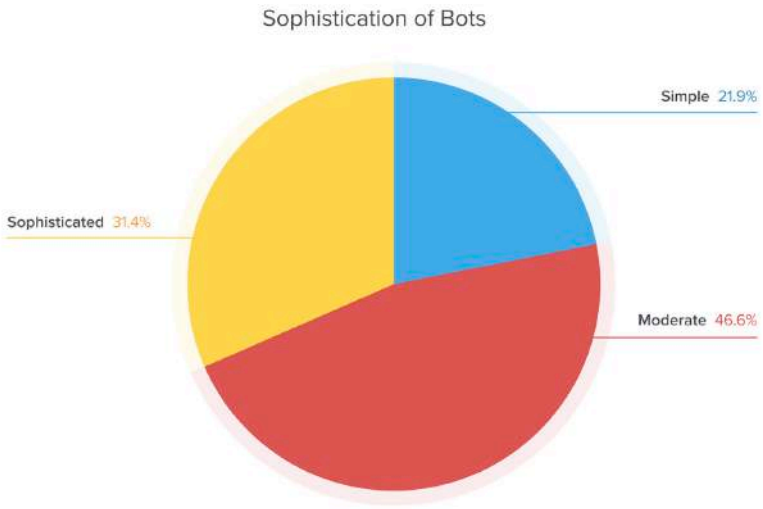
Nearly a third (31.4 percent) of the bots on ticketing platforms we studied were classified as sophisticated. Only 21.9 percent were simple bots. The remaining 46.6 percent were moderately sophisticated.

Bot Sophistication	Ticketing Domains 2017[1]	Ticketing Domains 2018
Sophisticated	19.10%	31.40%
Moderate	59.63%	46.60%
Simple	21.27%	21.90%

Mobile Versus Desktop

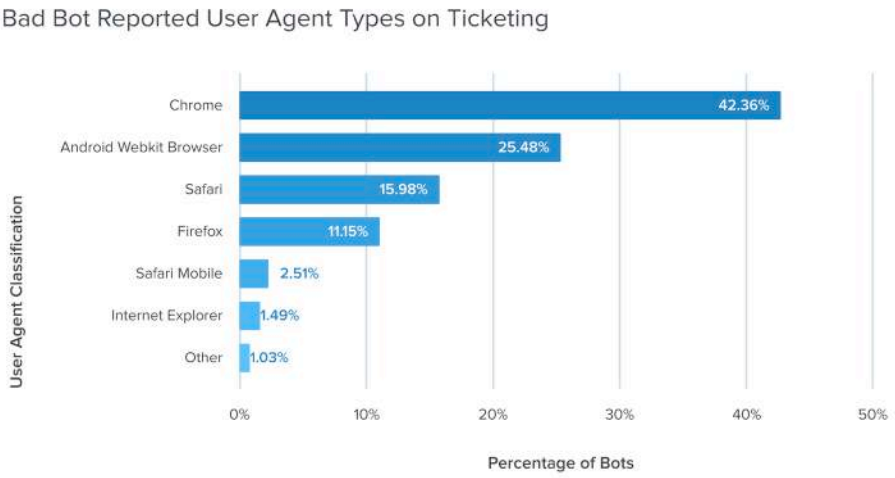
About seventeen percent of all bad bots on ticketing platforms identify as originating from a mobile device. That's high in comparison to other industries. The rest (82.9 percent) all claim a user agent associated with a desktop browser. While this proportion of mobile impersonators is still less than one in five, it is consistently growing and this trend is expected to continue.





Top Self Reporting Browsers

Across all ticketing domains, bad bots identified themselves as one of 432 unique user agents. In common with other industries, a high proportion (42.36 percent) of all bad bots claim to be Chrome. Clearly, ticketing bots are still attempting to hide in plain sight by impersonating the most popular browser. Unlike other industries, Android mobile browser is the second most popular identity claimed by 25.48 percent of bad bots. This is another example of ticketing leading the way and suffering from abuse by the most sophisticated of bots—more of them are adopting mobile identities. Safari mobile makes up 2.51 percent while Internet Explorer is only used by 1.49 percent of bad bots.



Bad Bots on Ticketing: A North America Problem

Eighty-five percent of the bad bots launched against ticketing companies originated in North America. (It should be noted that North American and European ticketing platforms comprise the majority of the data in this study.)

The United States is the leading source of bad bots on ticketing domains and is responsible for 67.01 percent of this traffic. This proportion dwarfs the contribution the U.S. makes across all industries; in the 2018 Bad Bot Report, the U.S. was responsible for 45.2 percent of all bad bot traffic.

Canada is responsible for the origination of 18.26 percent of bad bots on ticketing platforms, and only 3.7 percent of bad bot traffic across industries.

Great Britain (2.15 percent), Italy (2.02 percent) and Germany (1.90 percent) round out the top five source-countries but are inconsequential compared with the U.S. and Canada.

Bad Bots on Ticketing: A North America Problem

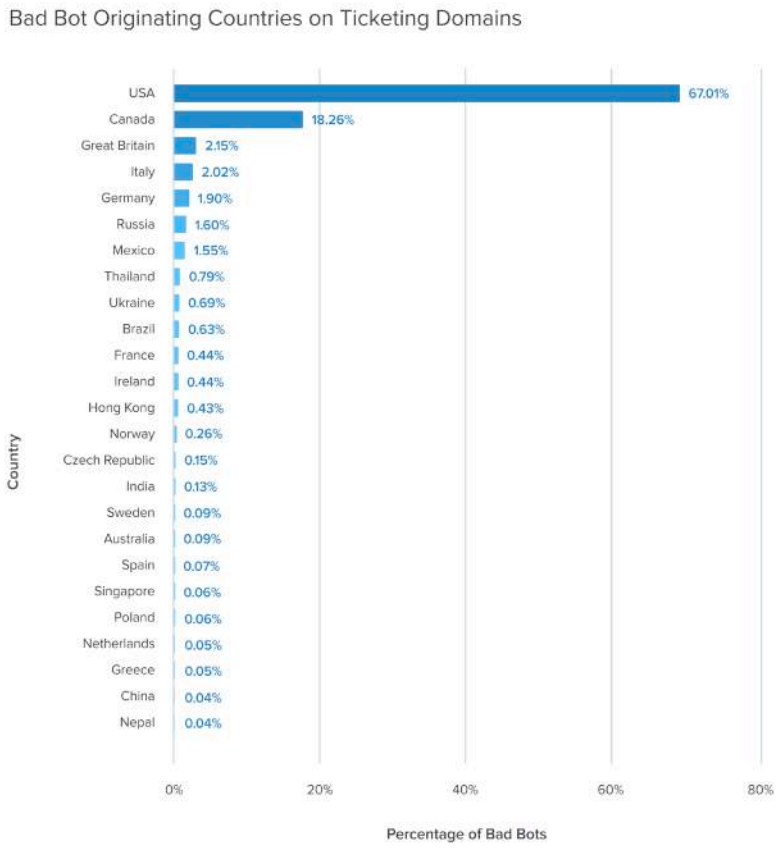
Eighty-five percent of the bad bots launched against ticketing companies originated in North America. (It should be noted that North American and European ticketing platforms comprise the majority of the data in this study.)

The United States is the leading source of bad bots on ticketing domains and is responsible for 67.01 percent of this traffic. This proportion dwarfs the contribution the U.S. makes across all industries; in the 2018 Bad Bot Report, the U.S. was responsible for 45.2 percent of all bad bot traffic.

Canada is responsible for the origination of 18.26 percent of bad bots on ticketing platforms, and only 3.7 percent of bad bot traffic across industries.

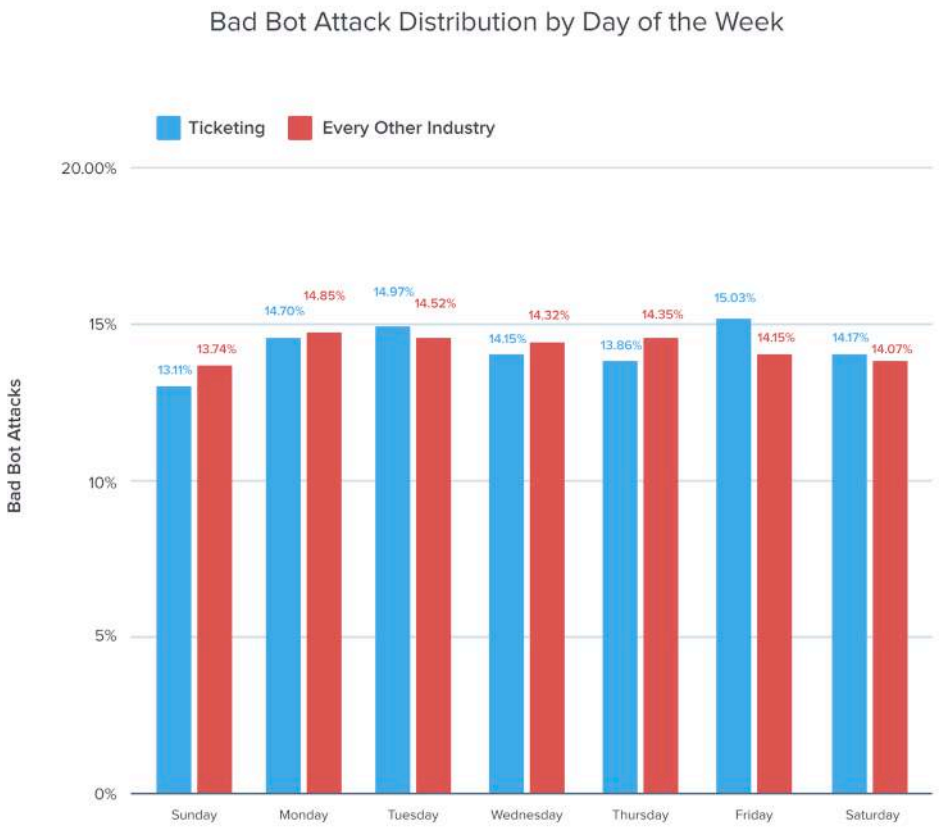
Great Britain (2.15 percent), Italy (2.02 percent) and Germany (1.90 percent) round out the top five source-countries but are inconsequential compared with the U.S. and Canada.

It is noteworthy that in our previous 2018 Bad Bot Report, China was responsible for 10.5 percent of bad bot traffic across industries, but is only responsible for 0.04 percent of bad bot traffic in the ticketing industry.



Ticketing Bots By Day of the Week

The consistency of bad bot traffic on ticketing domains is noticeable when examining the data by day of the week. Bots don't sleep and work around the clock, every day of every week. In other industries, such as airlines, there are small peaks of bot traffic on Friday. But on ticketing domains, there is no significant variance by day of the week.

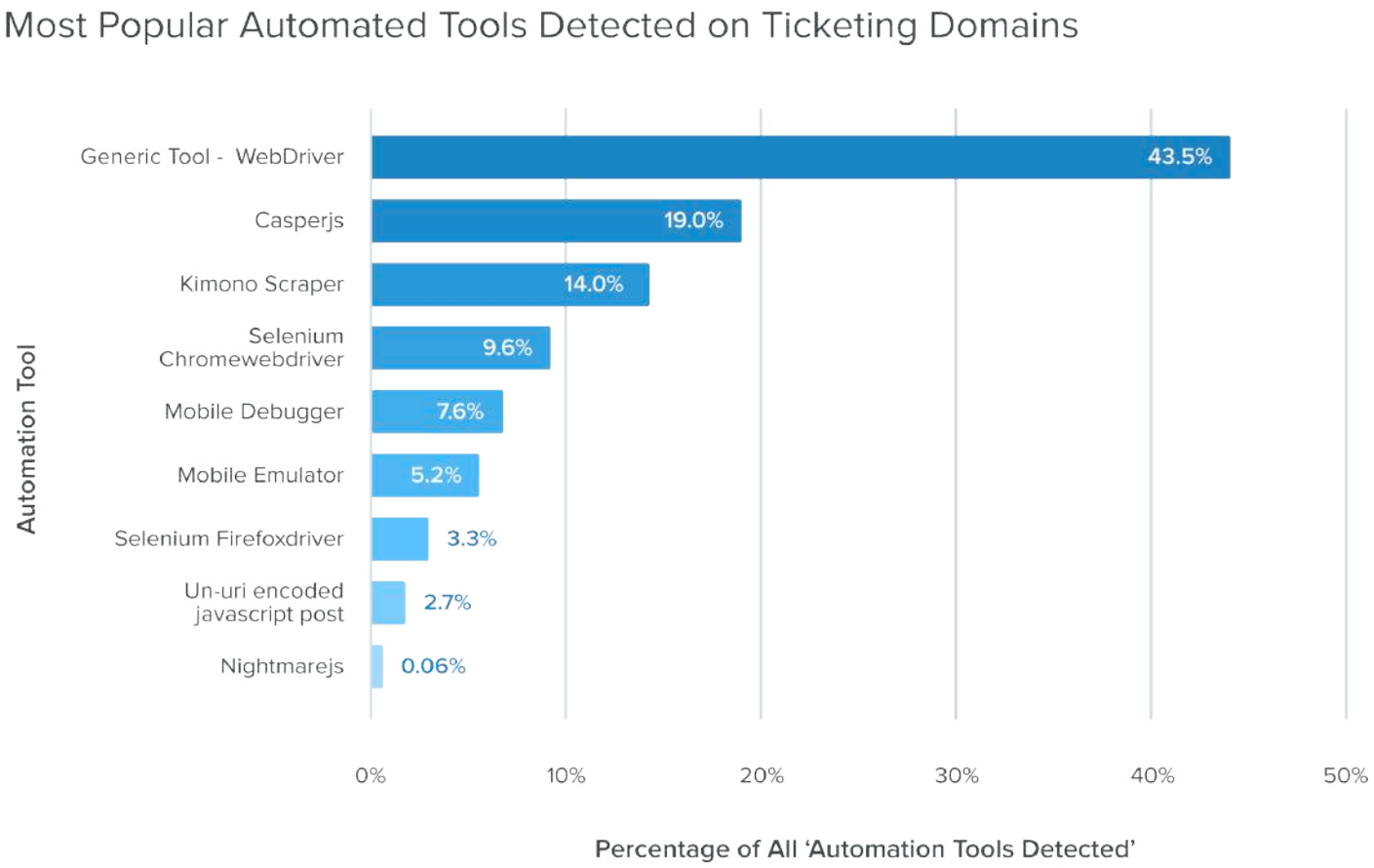


Popular Automated Tools Used on Ticketing Domains

Of the bad bots identified as an automated tool, a generic automation framework (WebDriver) was the most popular accounting for 43.5 percent of those detected. Casperjs and Kimono Scraper were the second and third most popular tools detected on ticketing domains.

Different versions of Selenium also saw significant usage—Selenium "Firefox" accounted for 3.3 percent and Selenium "Chrome" accounted for 9.6 percent.

Mobile tools were also detected. Mobile debuggers accounted for 7.6 percent of automated tools and mobile emulators were 5.2 percent, which further indicates the increasing part that mobile bots are playing in attacking ticketing companies which use mobile apps.



Recommendations for Detecting Bad Bot Activity

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

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:
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.

BROWSER VERSION	BLOCK End of life more than 3 years	CAPCHA End of life more than 2 years
Firefox Version	<38	<45
Chrome Version	<41	<49
Interent explorer	<10	10
Safari Version	<9	9

- Block these data centers:
- Digital Ocean
- DigitalOcean
- OVH SAS
- Choopa, LLC
- OVH Hosting
- GigeNET
- Amazon.com

1. Protect every bad bot access point: 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.
2. Carefully evaluate traffic sources: Monitor traffic sources carefully. Do any have high bounce rates? Do you see lower conversion rates from certain traffic sources? These can be signs of bot traffic.
3. 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.
4. 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.
5. 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.
6. 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.

7. 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.