distil networks

DISTIL RESEARCH LAB

Threat Research

HOW BOTS AFFECT TICKETING

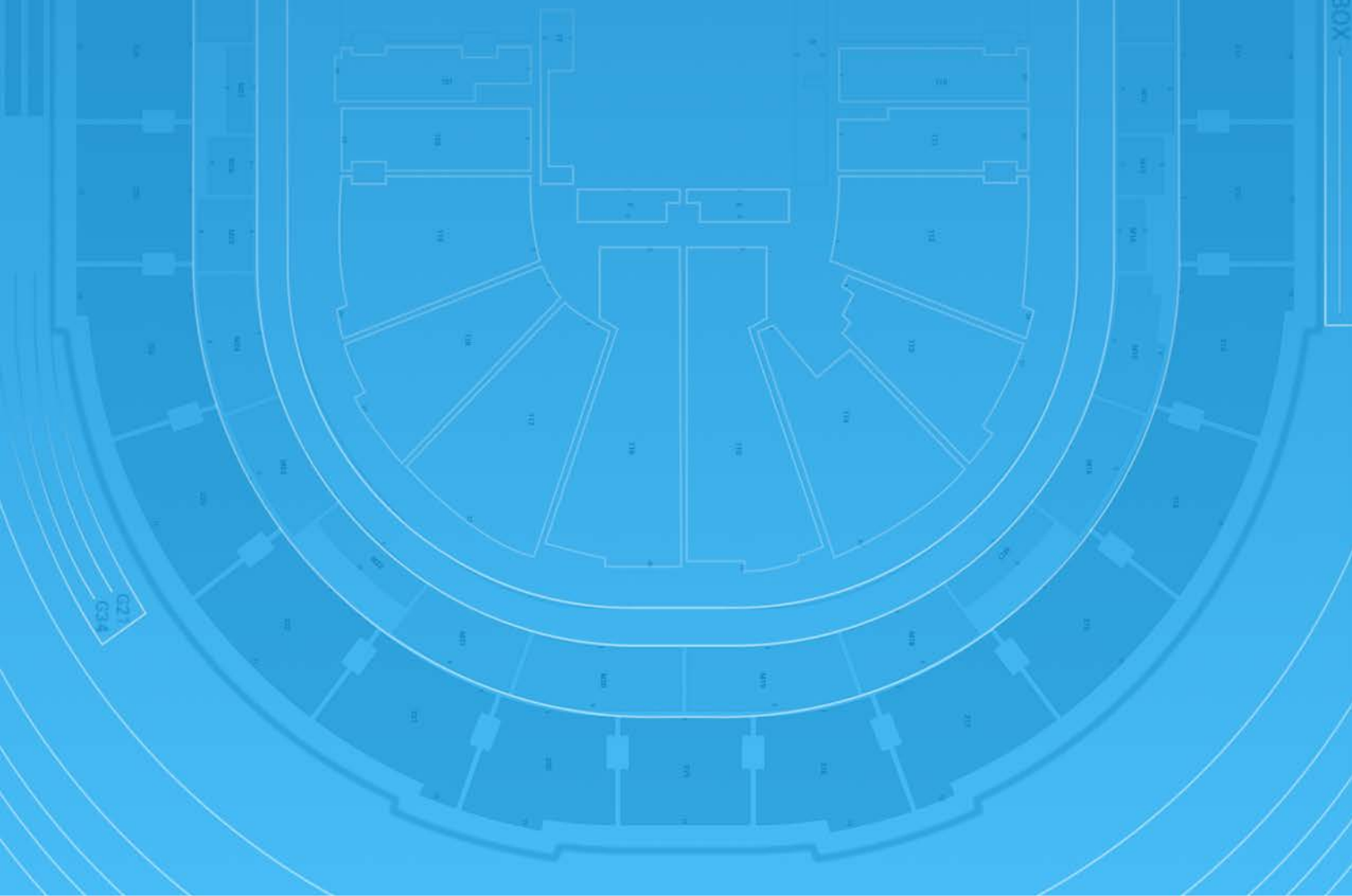


Table of Contents

Executive Summary of Findings

Bots By The Numbers

Bad bot traffic percentage - All industries	**21.8%**[1]
Bad bot traffic percentage - Ticketing	**39.9%**
Highest bad bot traffic percentage on an ticketing domain	**99.96%**
Number of ticketing domains with greater than 40% bad bot traffic	**32**

Five Groups Attack Ticketing With Bots

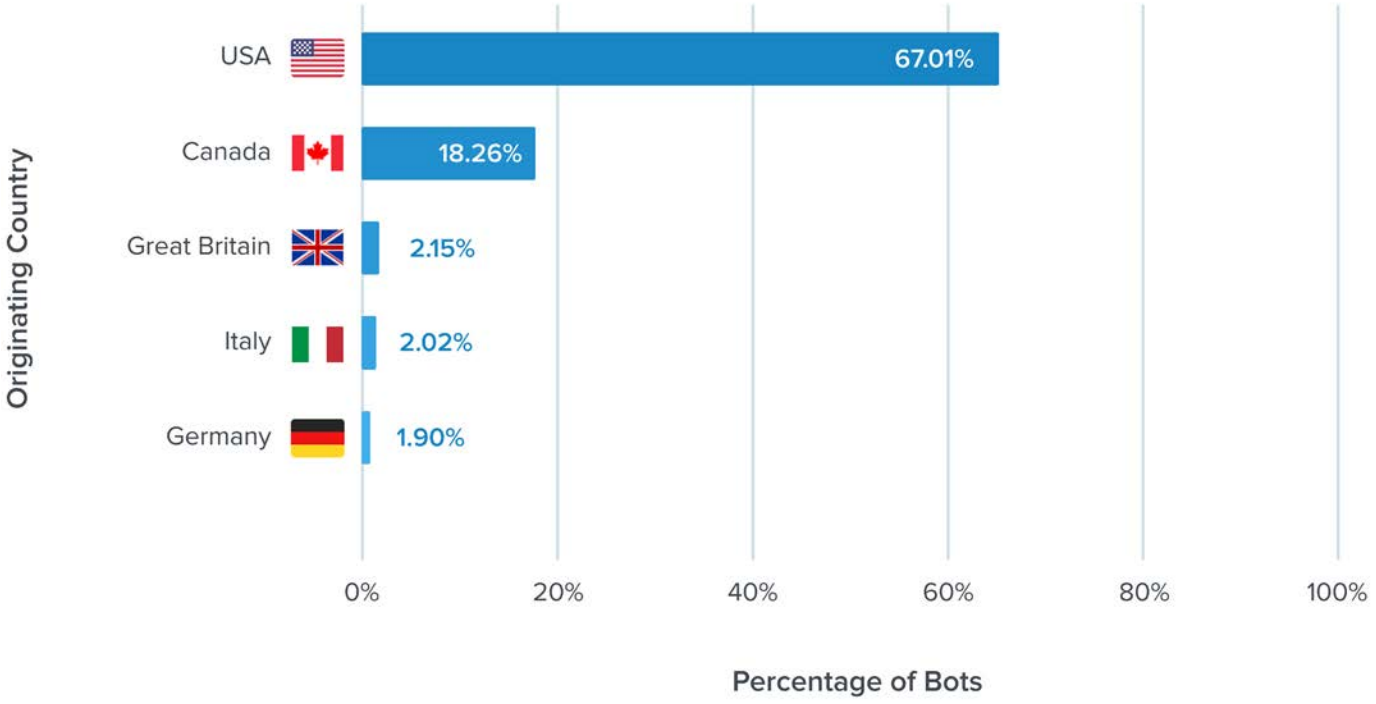
Who Launches Bots	Bot Objectives
Brokers	Scrape ticket details Instantly purchasing any available tickets to re-sell (Scalping) Continuously checking seat map inventory for newly released seats
Individual Scalpers	
Hospitality Agencies	Scrape ticket details Instantly purchasing best available tickets to re-sell Continuously checking seat map inventory for premium seats
Corporations	
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

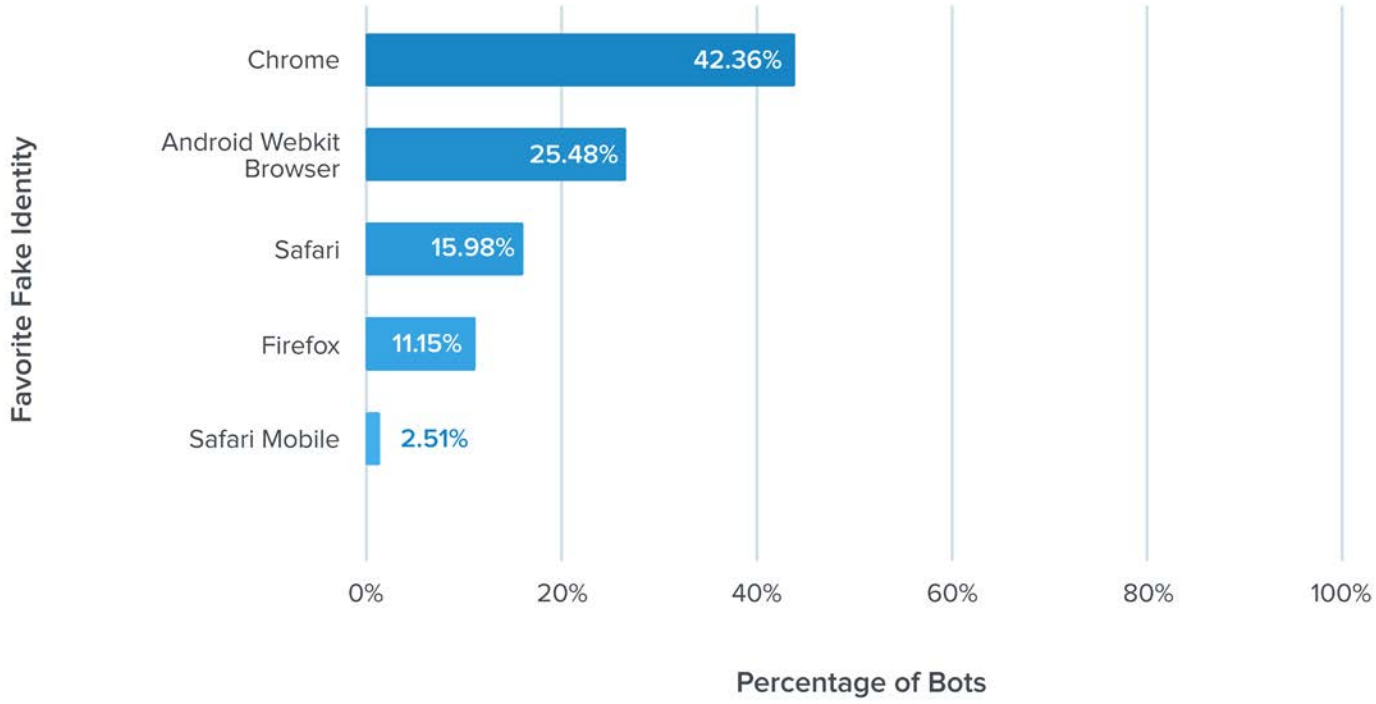
Bot Sophistication	Ticketing Domains 2017 [1]	Ticketing Domains 2018
Sophisticated	19.10%	31.40%
Moderate	59.63%	46.60%
Simple	21.27%	21.90%

[1] 2018 Bad Bot Report: The Year Bad Bots Went Mainstream

TOP 5
Ticketing Bot Traffic Originating Country

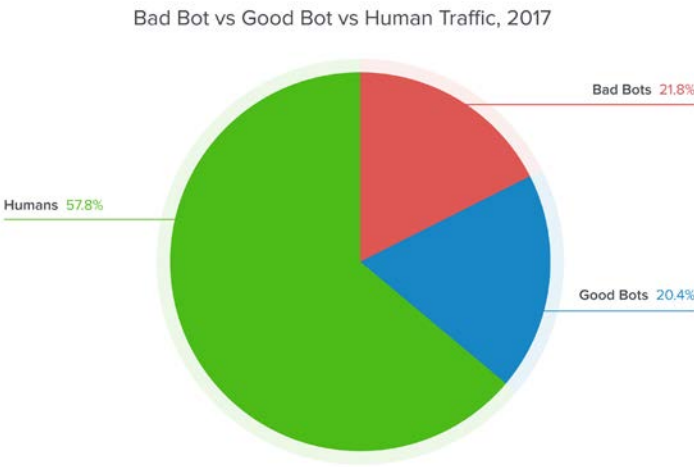


TOP 5
Ticketing Bots Favorite Fake Identity



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% of web traffic is actual humans—the rest are bots. While some bots are welcomed by businesses, like search engines, there are other nefarious bots which are unwanted and are dangerous to the success of the organization. These bad bots comprise 21.8% of all web traffic[2].

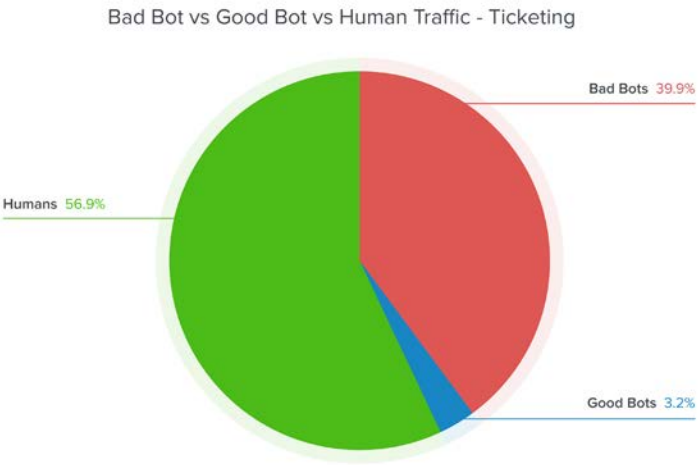


The Ticketing Bot Problem

The ticketing industry bad bot problem is unique. In previous bad bot reports the proportion of bad bots amongst ticketing companies was 22.97%[3], which was worse than the average for all industries but in this new study this number has risen to 39.9% of all traffic. This increase is explained by the greater number of ticketing companies included in the study and the increase in volume of traffic analyzed making the dataset more robust.

Interestingly, the proportion of human traffic is very similar to the average seen across all industries. The major difference is within the composition of bot traffic. There are far more bad bots (39.9%) compared with good bots (3.2%) on ticketing domains. This lower proportion of good bots is explained in two ways.

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



2/3 2018 Bad Bot Report: The Year Bad Bots Went Mainstream

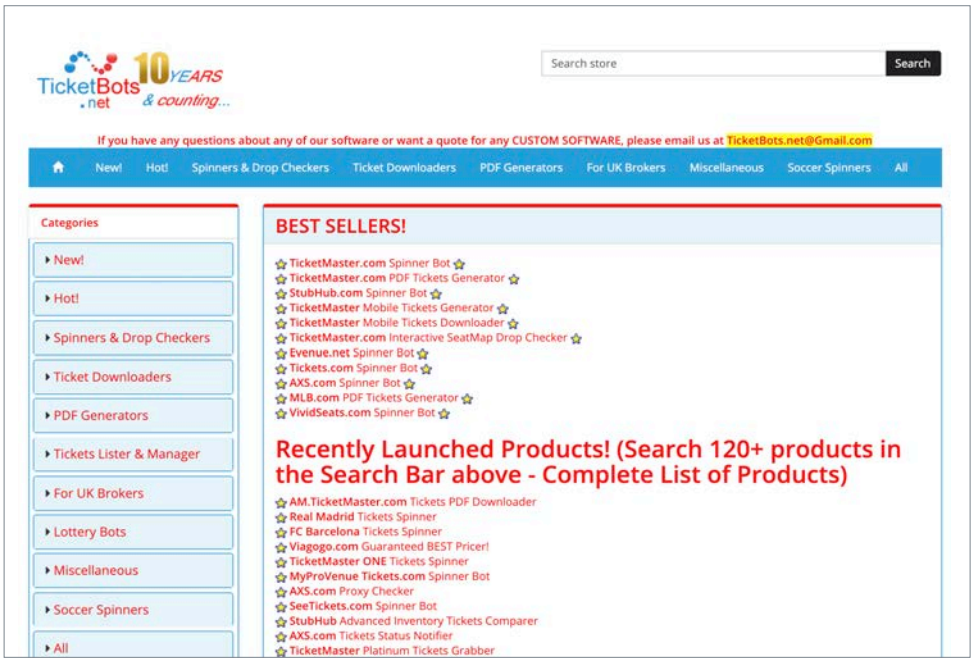
Historically, ticketing has led the way in the evolution of the bot problem. As the ticketing industry moved online, it was the first industry to suffer from nefarious bot operators using automated attacks to hold and scalp tickets. Following customer complaints, and increased pressure from artists, it was also the first industry to adopt legislation as an additional tool in the war on bad bots. In the USA, the 2016 Better Online Ticket Sales Act (commonly known as the BOTS Act) outlawed the resale of tickets purchased using bot technology complete with fines for any 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 many fans looking to attend a show by their favorite artist have experienced frustration and were unable to purchase a ticket online, it is also appropriate to understand the problem from the ticket platform's point of view. To fully grasp the scale of the around-the-clock battle that ticketing companies fight everyday, consider there are ecommerce businesses like ticketbots.net selling malicious bots to anyone looking to take advantage of any ticketing platform. A quick scan of its homepage shows the multitude of bad bots available for purchase including which ticketing platforms they exploit, and even the specific sports teams they target.

This is the environment that primary ticket platforms work in every day. Demonstrating the unrelenting nature of the problem, the website even offers to provide "quotes for any CUSTOM SOFTWARE" (see immediately below the ticketbots.net logo). This means that 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 and damage the real fan's experience.



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, which type of bot operator is using them, and what is the business impact on ticketing companies.

Ticketing Web Property Structure

At the heart of the bot problem is the ticketing website and mobile app. This is the online home for all event information which is presented for customers to make purchase decisions, including seat availability at different pricing tiers, payment processes, and different methods of delivery for purchased tickets.

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

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

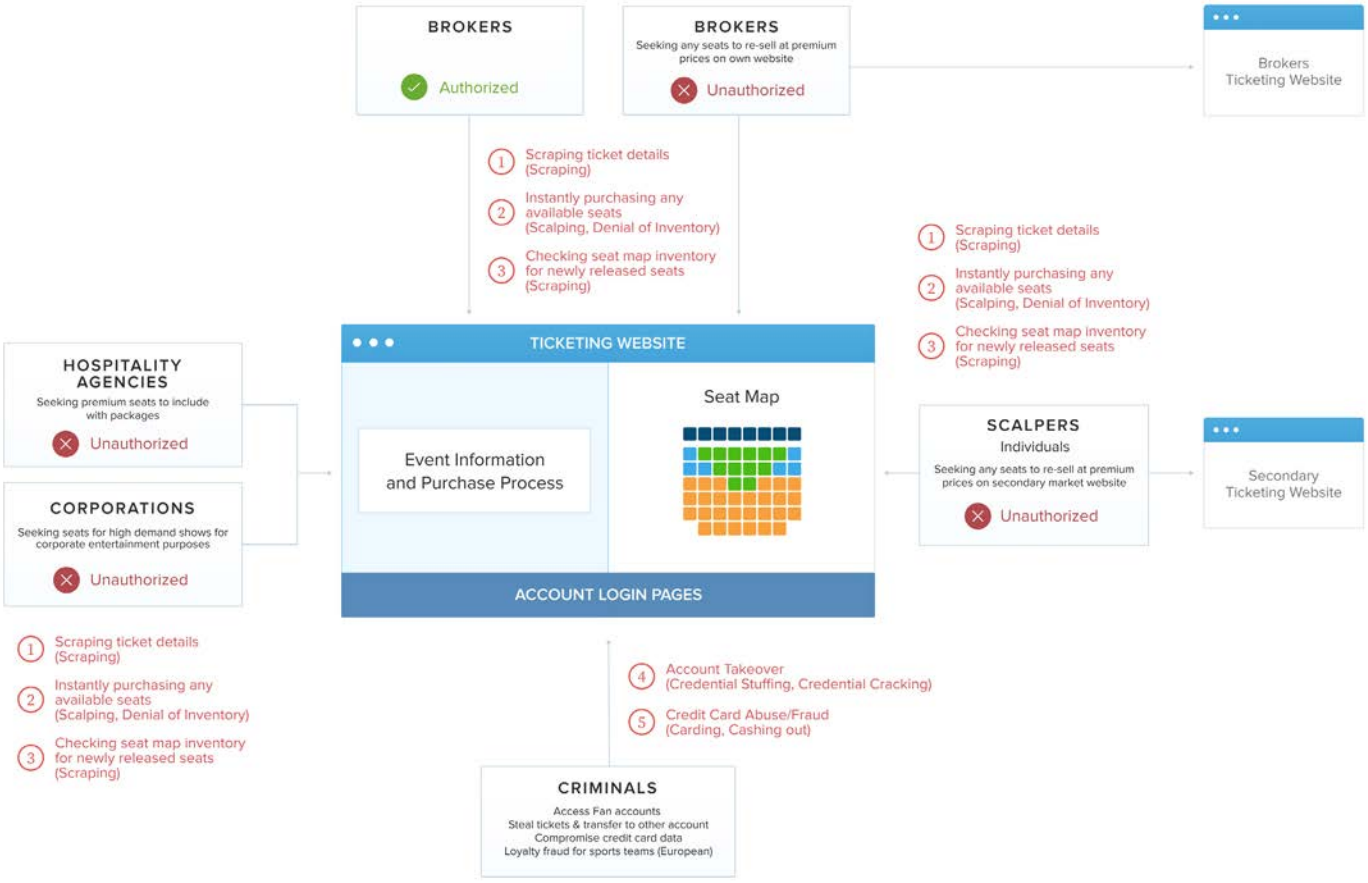
Regardless of the specific technical structure of the website, consistent problems plague all ticketing platforms in the shape of bots. In general, they are launched from five main groups of bot operators.

Bot Operators: Brokers

Brokers are a channel that distributes and sells tickets to fans to attend concerts and sports events 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 any associated fees. To understand the supply and demand of an onsale, 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 (aka 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 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 (aka touts) are running a business using similar techniques to brokers but at a smaller scale. Scalpers deploy bots to hold or purchase seats made available at the start of an onsale with the goal of reselling or scalping the tickets on the secondary market. The difference from brokers is that they don't use their own website to resell the tickets, instead they use any of the popular secondary market ticketing platforms. 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 shows or events. These corporations use these tickets for corporate entertainment purposes as perks for their clients or executives.

Bot Operators: Criminals

Primarily, criminals launch bots at ticketing platforms aimed at compromising fan or customer accounts. Bots are used in brute force credential stuffing and credential cracking attacks with the goal of gaining access to any fan accounts. By running stolen credentials against the login pages of ticketing platforms, bots identify those accounts where access was granted. Once inside the account, any stored tickets can be stolen or transferred to another account. Furthermore, once inside an account any stored credit card and personal information could be stolen or used to commit fraud. Secondarily, credit card fraud like card cracking is also performed by bots. Access to fan accounts exposes the possibility of fraud from loyalty programs offered by some sports teams within their season ticket programs. This is more prevalent with season ticket holders in European soccer.

Account takeover shakes the confidence of the fan so much that many will no longer use the ticketing platform. Once an 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. In addition, there is the cost of reimbursement any theft or credit card fraud.

How Bots Affect Ticketing

Ticketing companies are in a constant war against bots. There are consistent business problems created that are caused by the continual barrage of bots. These include 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 the customer experience of real fans and ultimately the reputation of the ticketing platform. But collectively, these bot activities can add up to a significant headache for the business and especially the IT team, and left unaddressed may 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, corporations to purchase any tickets within milliseconds of them going on sale, it creates fan frustration for those real humans unsuccessfully using the website or mobile app to purchase tickets. These bad bots create a denial of inventory problem for the real fan. But instead of criticizing the bots, it's typical for frustrated fans to blame the ticketing platform and its reputation is diminished with every failed attempt. Furthermore, vocal fans using social media are making their frustration known to artists who are increasingly taking up the mantle to 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 the 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 a primary market, will quickly turn to secondary ticketing marketplaces or broker websites, and have their frustration exacerbated when they see tickets at premium prices considerably higher than face value. 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 higher on primary ticket markets. The numbers of scalpers found on secondary market websites is considerably less 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

For many shows, tickets are released at different times. Bots are used by brokers, scalpers, hospitality agencies, and corporations continually to check when new seats are available. For high demand shows, premium seats 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.

Accessing Fan Accounts

Criminals use bots to perform account takeover of fan accounts. Once inside the account, any tickets inside the account can be stolen or transferred to another account. A noticeable spike in requests to a login page combined with a rise in the typical proportion of failed login attempts is a key indicator that an account takeover attack is underway.

Accounts on secondary ticketing websites are targeted more often because they hold both tickets that are being sold and any currency or credits exchanged in the sale of tickets.

In Europe, the theft of loyalty points associated with accounts owned by season ticket holders of many soccer teams is also a concern of ticketing platforms. An increase in complaints about loss of loyalty points is another indicator of increased bot activity resulting from account takeover.

Fraud: A Cost of Doing Business?

Credit card fraud is a constant problem for any ecommerce 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 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.

BOT ACTIVITY	TICKETING IMPACT
1 DENIAL OF INVENTORY	Real fans locked out of buying tickets Fan frustration leads to brand damage Lost customers when they purchase on secondary market Lost future revenue from lack of brand loyalty Artist frustration resulting from negative fan feedback
+	
2 SPINNING AND SCALPING	Real fans unable to buy seats at face value Helps create the secondary market Fans pay premiums over face value per ticket Brand damage Artist worries fan being exploited
+	
3 SCRAPING SEAT MAP INVENTORY	Real fans locked out of buying newly released tickets Real fans locked out of buying premium tickets High volume of bot requests Increased infrastructure required to maintain uptime
+	
4 FAN ACCOUNT TAKEOVER	Angry fans, higher customer service costs, forensic investigations, reimbursement costs, customer retention problems Brand damage
+	
5 FRAUD (CREDIT CARD)	Angry fans, higher customer service costs, forensic investigations, reimbursement costs, customer retention problems Brand damage
=	
6 HIGHER INFRASTRUCTURE COSTS	Poor website performance Application denial of service or slowdowns giving poor customer experience Skewed analytics (Conversion rates, A/B tests of current offers) lead to poor decisions

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 an aggregate of data gathered and is not intended to reveal the data for any specific company.

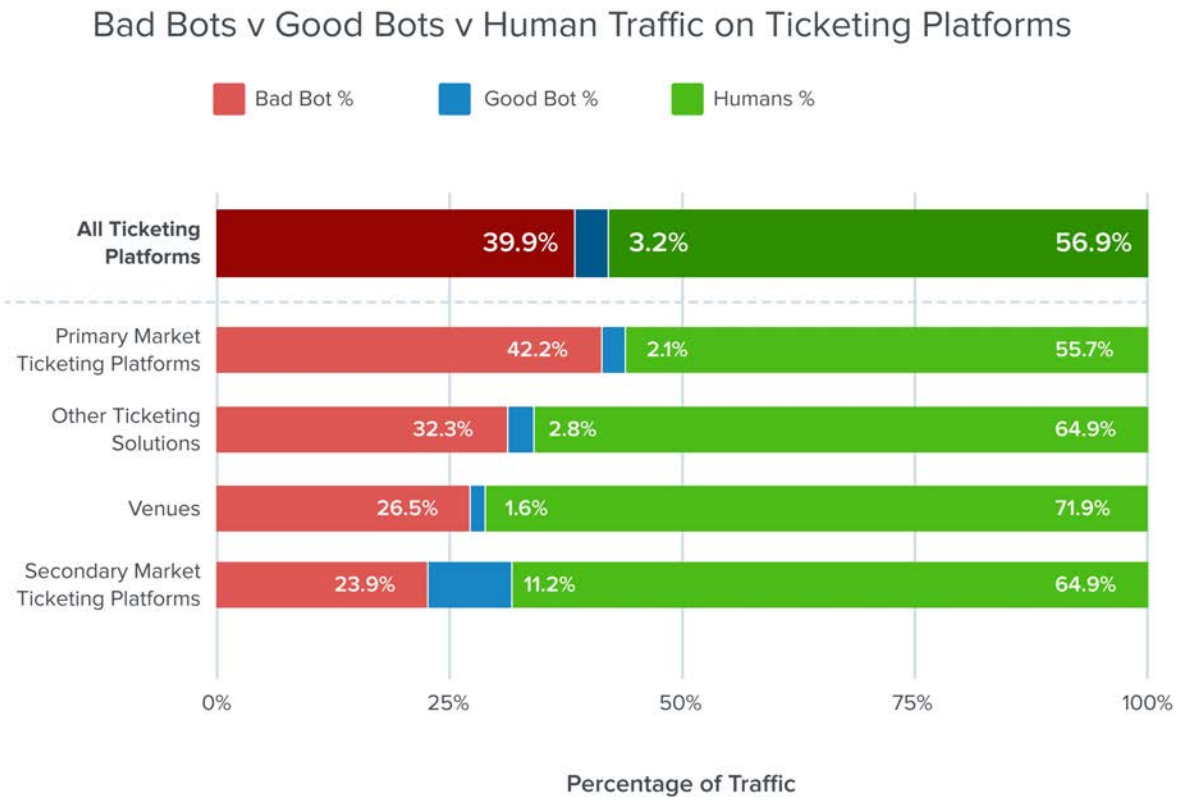
Number of Domains	**180**
Time Period	**105 Days**
Date of Data Gathering	**Sep-Dec 2018**
Number of Requests Analyzed	**26.3 billion**

The Bots on Ticketing Platforms

Across all 180 ticketing domains, 39.9% of traffic is bad bots. The primary market ticketing platforms, where tickets are first made available, suffer the most with 42.2% of 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%) and see far less scalper bots but instead have a significant problem with credential stuffing and credential cracking bots looking to perform account takeover.

For venues, 26.5% of traffic is bad bots. For any other ticketing solution website that does not fall into primary, secondary market, or venues, the bad bot traffic is 32.3%.

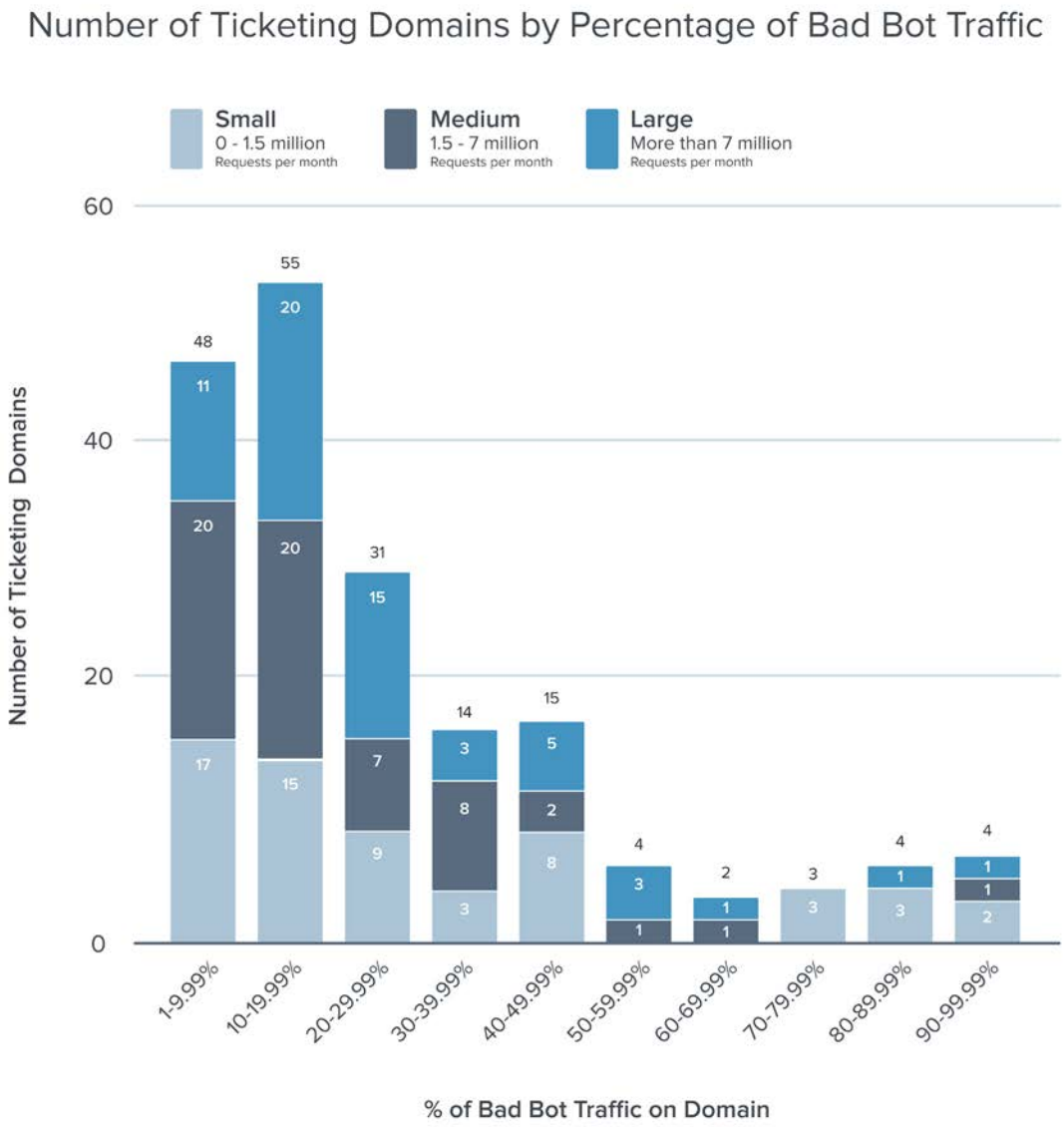


How Bad is Bad?

The domain identified as suffering from the highest proportion of bot traffic was on a secondary market ticketing platform—99.96% of its traffic was bad bots. Humans accounted for only 0.03% of its traffic.

On 32 of the domains, the bots accounted for greater than the 40% of all traffic.

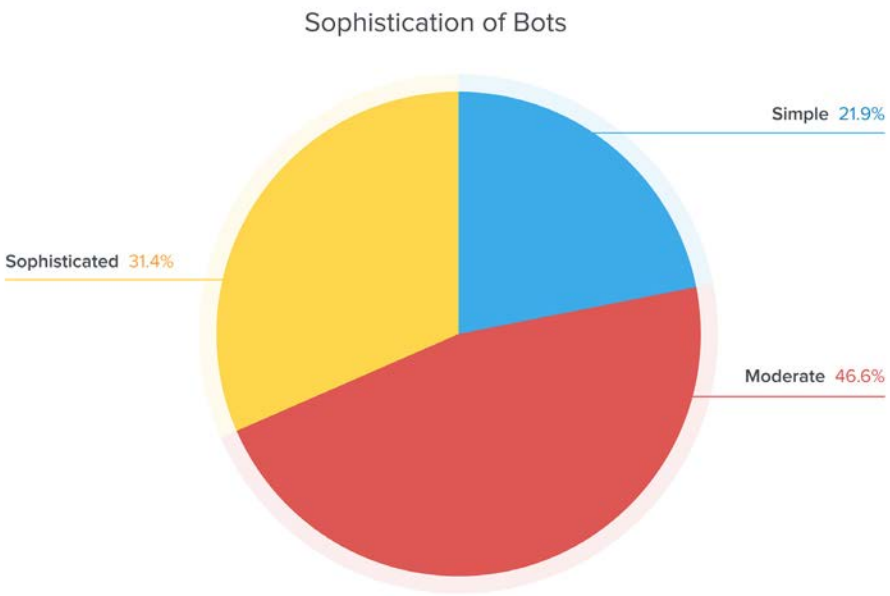
The amount of bad bots seen is 21.8%[4] across all industries. In this study, 70 ticketing domains exceed this proportion of bad bot traffic.



[4] 2018 Bad Bot Report: The Year Bad Bots Went Mainstream

Ticketing Bot Sophistication Rises

Nearly a third (31.40%) of bots on ticketing were classified as sophisticated. Only 21.90% were simple bots. The remaining 46.60% were moderately sophisticated.



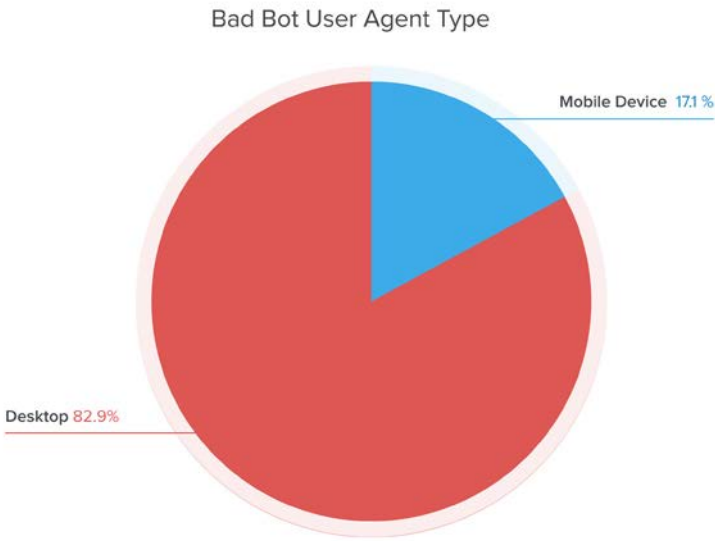
The sophistication level of bots on ticketing platforms is significantly higher than previously seen in the 2018 Bad Bot Report. In that research, 19.1% of bots on ticketing were sophisticated compared with 31.4% now. The volume of simple bots is similar, while there has been a drop in the percentage of moderate bots seen on ticketing platforms. This increasing sophistication is explained by the arms race at play between bot operators and bot detection technology. Once bots are detected and blocked, the challenge to the bot operator is to create another bot to achieve the same goal. Because the financial viability of brokers and individual scalpers is based upon bots scraping primary market ticketing data, the cycle continues ad infinitum.

Bot Sophistication	Ticketing Domains 2017[5]	Ticketing Domains 2018
Sophisticated	19.10%	31.40%
Moderate	59.63%	46.60%
Simple	21.27%	21.90%

[5] 2018 Bad Bot Report: The Year Bad Bots Went Mainstream

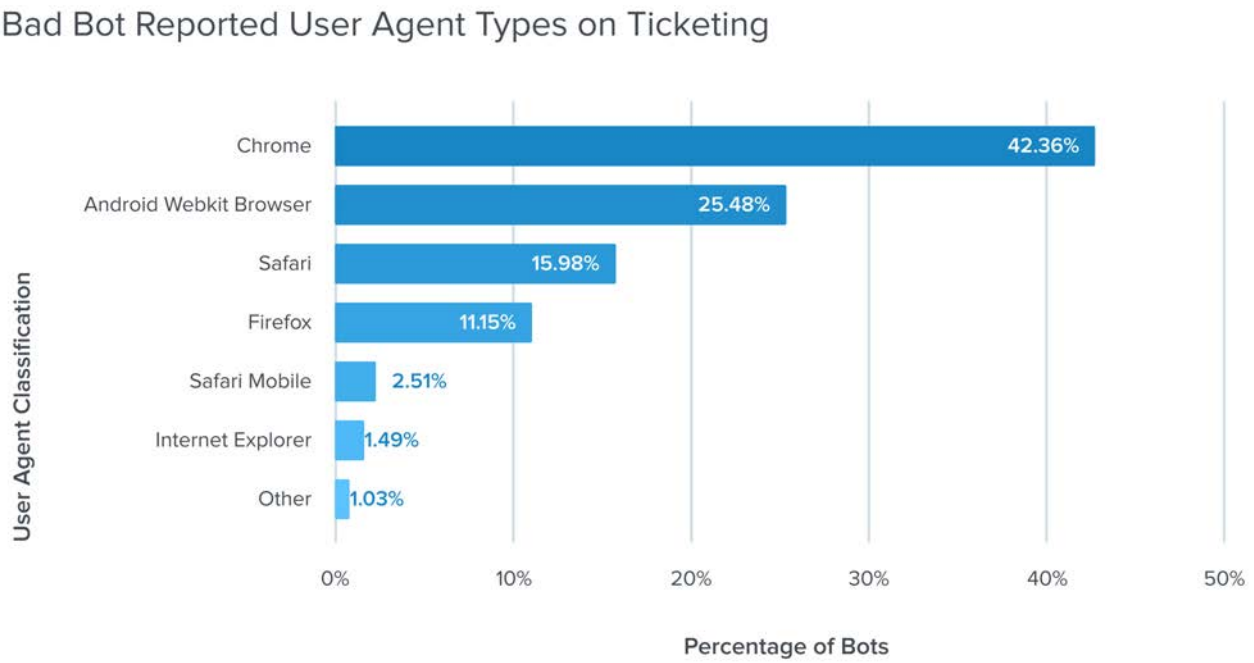
Mobile versus Desktop

More bots identify as user agents from mobile devices in ticketing compared with other industries—17.10% of all bad bots identify as originating from a mobile device. The rest (82.90%) 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%) 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% 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% while Internet Explorer is only used by 1.49% 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 data in this study.)

USA is the leading source of bad bots on ticketing domains and is responsible for 67.01% of this traffic. This proportion dwarfs the contribution the USA makes for all industries—in the 2018 Bad Bot Report, USA was responsible for 45.2% of all bad bot traffic.

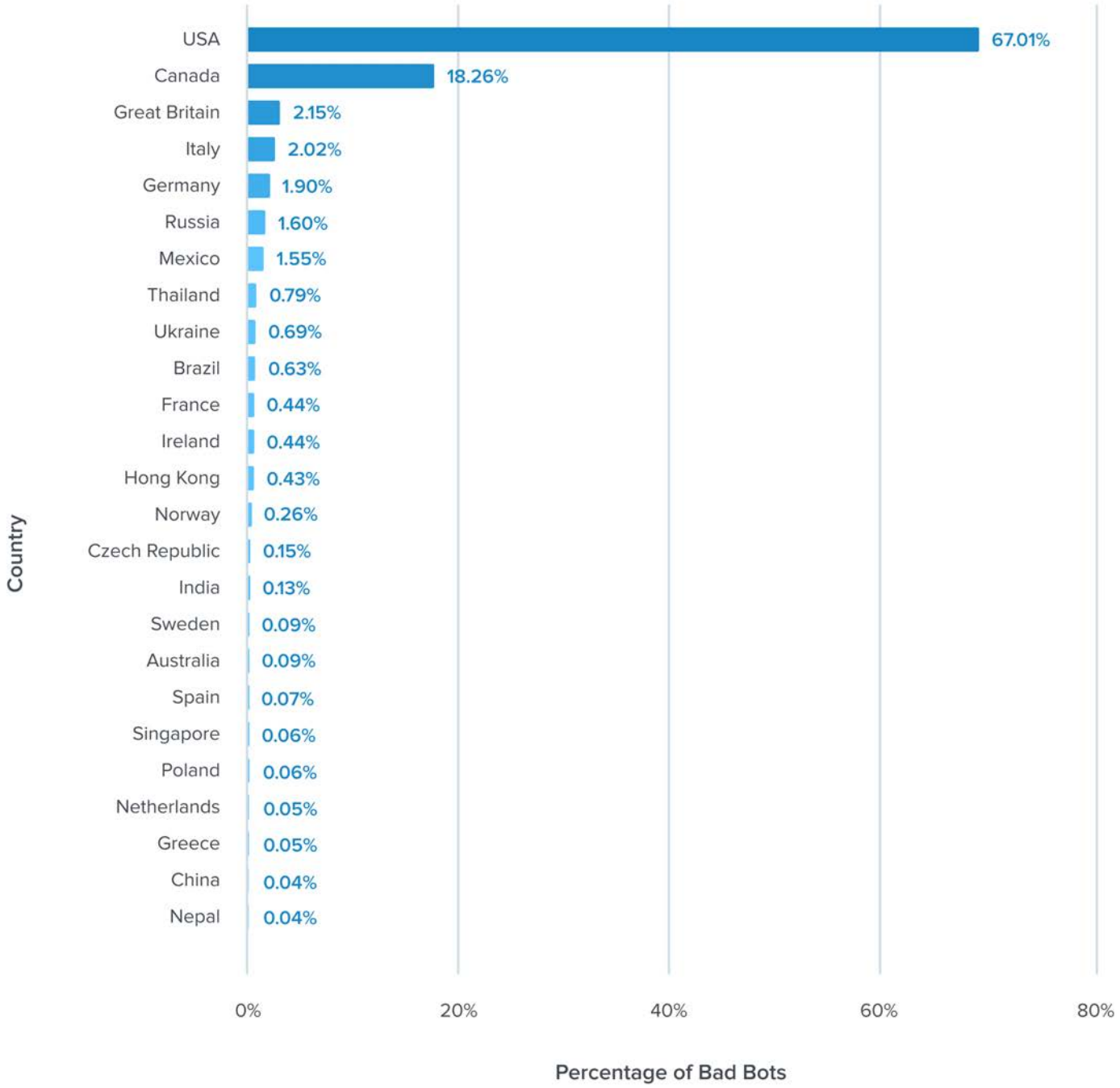
Canada is responsible for the origination of 18.26% of bad bots on ticketing platforms. As a comparison with all industries, Canada was previously responsible for only 3.7%[6] of bad bot traffic.

Great Britain (2.15%), Italy (2.02%) and Germany (1.90%) round out the top five but are inconsequential compared with Canada and the USA.

Noteworthy is that previously in the 2018 Bad Bot Report, China was responsible for 10.5% of bad bot traffic seen, but on ticketing companies in this study it comprises of only 0.04% of bad bot traffic.

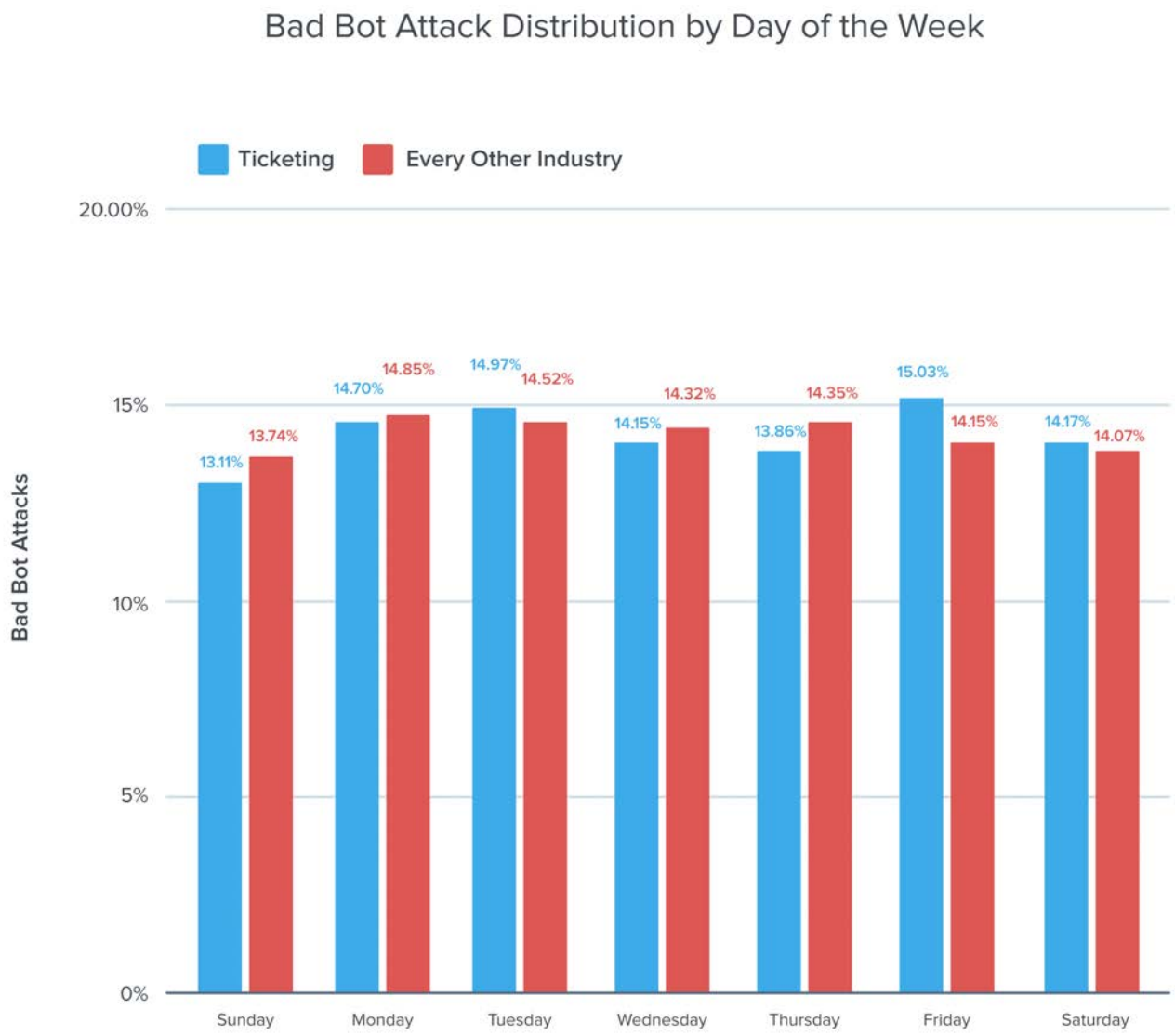
[6] 2018 Bad Bot Report: The Year Bad Bots Went Mainstream

Bad Bot Originating Countries on Ticketing Domains



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 they are working around the clock, every day of the week. In other industries, like airlines there are small peaks of bot traffic on Friday. But with ticketing domains, what is remarkable is that there is no significant variance by day of the week. Ticket companies know that bots are busy everyday.



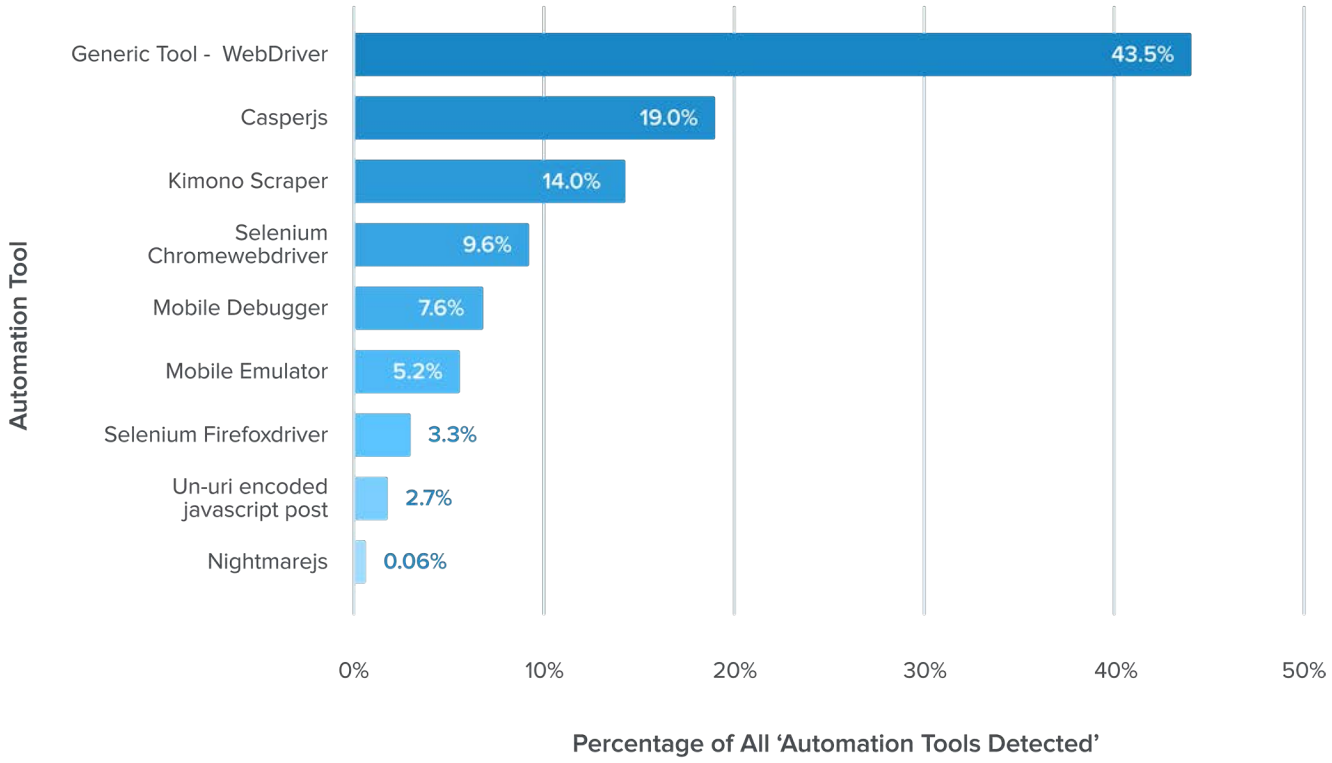
Popular Automated Tools Used on Ticketing Domains

Of the bad bots identified as an “Automated Tool”, a generic automation framework (WebDriver) was the most popular accounting for 43.5% 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” with 3.3% and Selenium “Chrome” with 9.6%.

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

Most Popular Automated Tools Detected on Ticketing Domains



Bots Perform Account Takeover

Bots run credential cracking and credential stuffing attacks to identify which pairs of usernames and passwords gain access to any accounts.

Credential cracking attempts. where the bot is programmed to try “common” passwords with stolen email addresses in what is known as a ‘dictionary attack’, are typically low and slow and occur consistently around the clock.

Credential stuffing is when a criminal runs a list of stolen paired credentials against sites around the world hoping to gain access, and is volumetric in nature. These attacks are spikey and last for a short period, but if they are large enough can cause slowdowns or downtime due of the demands placed on the backend database during repeated authentication attempts.

The typical range of volumetric account takeover attacks is 2-3 per month. [7]

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 the login page combined with a higher than normal failed login rate is an indicator of account takeover attempts by bots.

[7] Threat Research: The Anatomy of Account Takeover Attacks

Recommendations

Bots are on ticketing websites every day, and attack characteristics become more advanced and very nuanced. 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:

BROWSER VERSION	BLOCK End of Life More than 3 years	CAPTCHA End of Life 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	OVH SAS	OVH Hosting	Choopa, LLC	GigeNET

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. **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.

8. **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. 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 this 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 on Distil, visit https://www.distilnetworks.com/block-bot-detection/ or follow @DISTIL on Twitter.