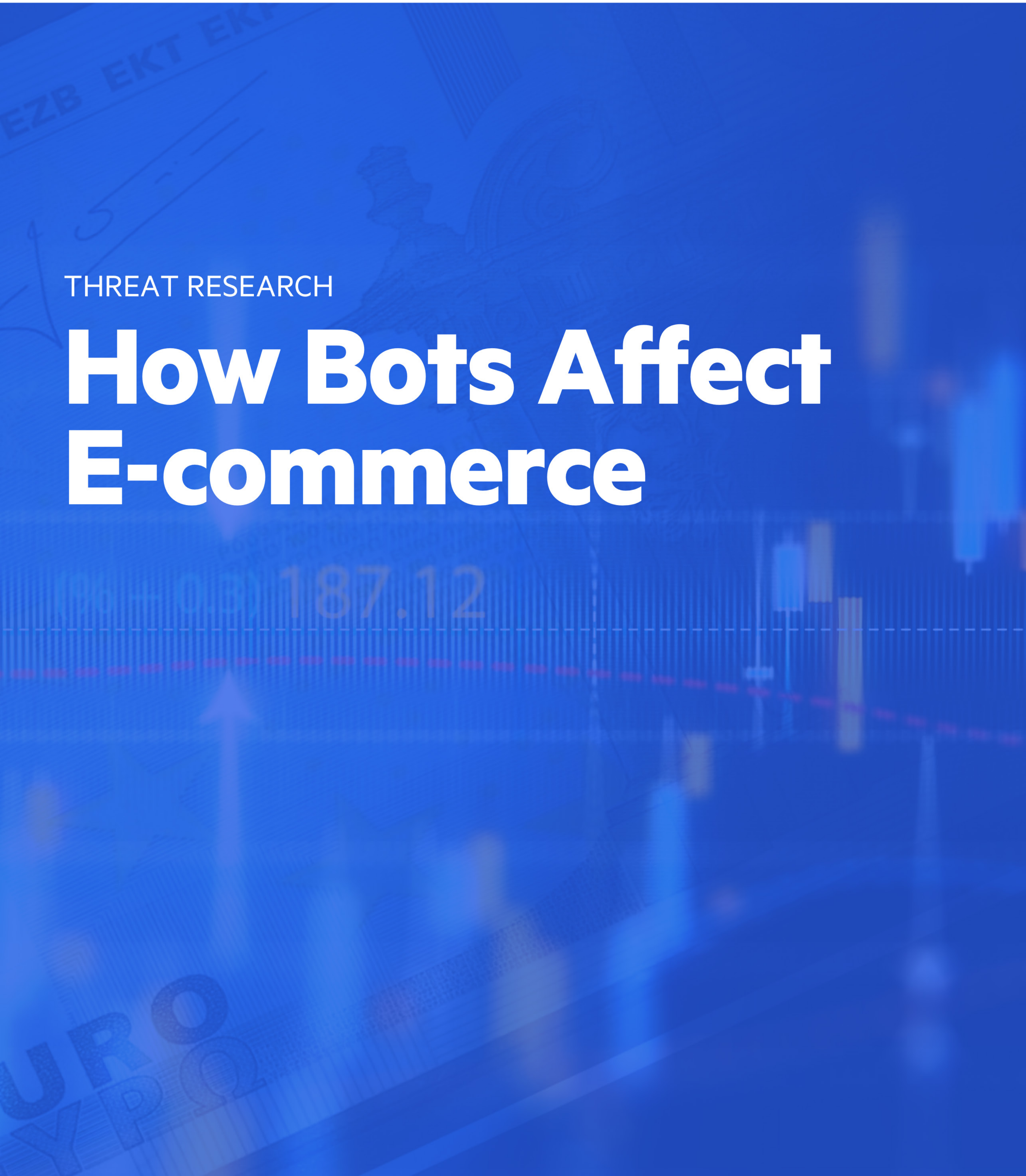


THREAT RESEARCH

How Bots Affect E-commerce

How Bots Affect E-commerce

TABLE OF CONTENTS

Executive Summary of Findings

Bots By The Numbers

BAD BOT TRAFFIC PERCENTAGE - ALL INDUSTRIES	20.4% [1]
BAD BOT TRAFFIC PERCENTAGE - E-COMMERCE	17.7%
HIGHEST BAD BOT TRAFFIC PERCENTAGE ON AN E-COMMERCE DOMAIN	99.15%
NUMBER OF E-COMMERCE DOMAINS WITH GREATER THAN 30 PERCENT BAD BOT TRAFFIC	77

Four Groups Attack E-commerce Businesses With Bots

WHO LAUNCHES BOTS	BOT OBJECTIVES
Competitors	Scrape comparative pricing to offer better price. Scrape market intelligence data for expansion into new markets.
Resellers	Scrape product information. Continuously check inventory of high demand items (e.g. Grinchbots) and limited edition items (e.g. Sneakerbots) to instantly purchase any available items.
Criminals	Account takeover to access customer accounts to commit fraud. Compromised accounts suffer from loyalty program fraud, loss of personally identifiable information, and credit card abuse. Gift card fraud.
Investment Companies	Scrape information to gather “alternative data” to determine the health of the business for investment purposes.

[1] 2019 Bad Bot Report: The Bot Arms Race Continues

Bot Sophistication on E-commerce Rises

BOT SOPHISTICATION	E-COMMERCE DOMAINS 2018[1]	E-COMMERCE DOMAINS 2019
Sophisticated	21.4%	23.5%
Moderate	54.4%	55.7%
Simple	24.2%	20.8%

Top 5 E-commerce Bot Traffic Originating Country

USA	63.6%
GERMANY	10.1%
FRANCE	6.2%
CANADA	5.5%
CHINA	4.9%

Top 5 E-commerce Bot Favorite Fake Identity

CHROME	66.0%
FIREFOX	13.6%
SAFARI	6.8%
SEM-RUSH	4.9%
ANDROID	2.2%

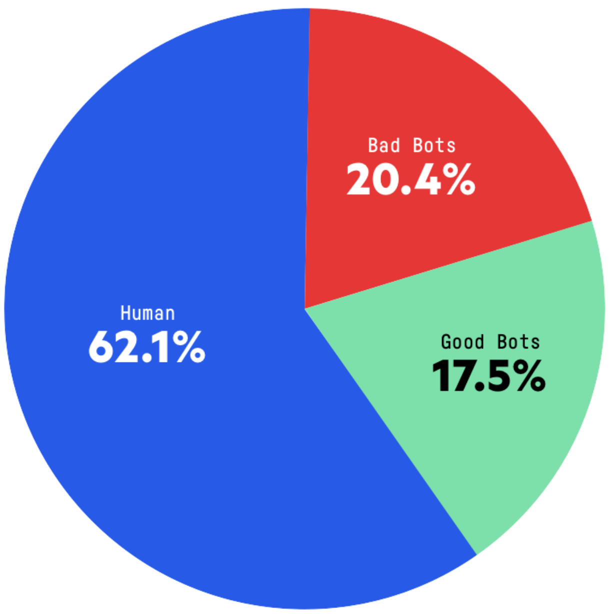
[1] 2019 Bad Bot Report: The Bot Arms Race Continues

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 62.1 percent of web traffic is generated by actual humans—the rest is bots. While some bots are welcomed by businesses, like search engines, there are other nefarious bots that are unwanted and dangerous. These bad bots comprise 20.4 percent of all web traffic[2].

> "Bad bots comprise 20.4 percent of all web traffic."
>
> 2019 BAD BOT REPORT:THE BOT ARMS RACE CONTINUES

Bad Bot vs. Good Bot vs. Human Traffic 2018



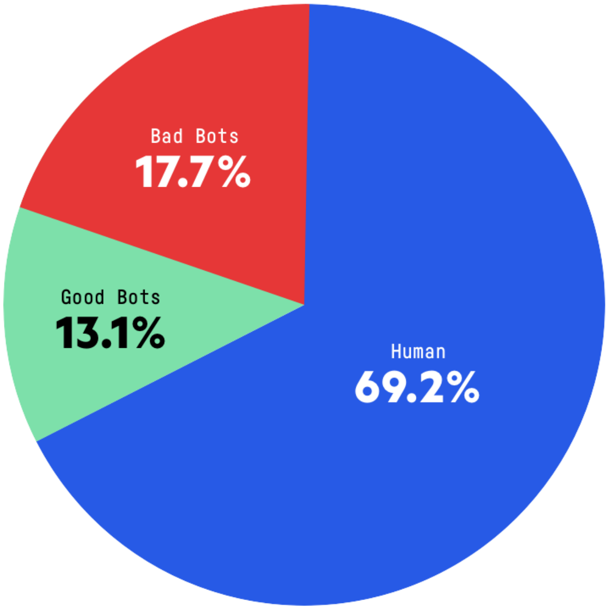
The E-commerce Bot Problem

The e-commerce industry suffers from a wide range of bad bot problems. The variety of bad bot attacks is more diverse in e-commerce than in many other industries. In previous bad bot reports, the proportion of bad bots amongst e-commerce companies was 18.0 percent[3], which was better than the average for all industries of 20.4 percent.

[2/3] 2019 Bad Bot Report: The Bot Arms Race Continues

In this new study, the proportion of bad bots is very similar at 17.7 percent of all traffic. The volume of humans remains steady at 69.2 percent while the volume of good bots is slightly higher at 13.1 percent. While the volume of bad bot traffic is not as high as other industries like ticketing or airlines, the functionality that bots abuse on e-commerce sites is more varied.

**Bad Bot vs. Good Bot vs. Human
E-commerce**



Legislation focused on the bot problem is still limited but is increasingly being proposed and enacted. 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.

Outside of the ticketing industry, the US Congress has also proposed the Stopping Grinchbots Act of 2018, which is focused on a specific bot problem faced by e-commerce retailers. Understanding the impact of this proposed legislation and how it will be enforced in a borderless internet is still unclear.

> **“The US Congress has also proposed the Stopping Grinchbots Act of 2018, which is focused on a specific bot problem faced by E-commerce retailers.”**

Website Availability and Conversion Rates Matter in E-commerce

In the ultra competitive environment of e-commerce, where similar products are only a click away on another website, converting a visitor to a customer is of paramount importance. E-commerce is focused on revenue from these conversions and understands the lifetime value of a satisfied customer. Unfortunately, in an environment where traffic is polluted by bots, metrics become difficult to believe and have a major impact on the accuracy of conversion rates.

Beyond analytics, aggressive scrapers and other bad bots potentially slow the website down, or worse, cause downtime. Poor performance and outages potentially force a customer to another site within seconds and the conversion is ultimately lost. Peak times like Black Friday, Cyber Monday, Cyber Week, or January Sales, when the volume of humans is at its highest, place a strain on infrastructure. It is vital to understand that any downtime in e-commerce equals lost revenue. Many e-commerce companies fail to consider the part that bots play in causing website availability and performance problems.

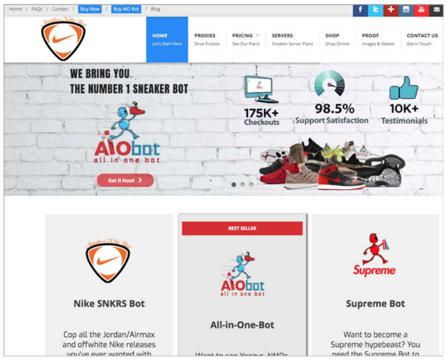
Don't Believe the Hype

Bots are not benign. They are on websites or mobile apps for a reason, and that reason is to make money. Anywhere there is money to be made, the adoption of technology can make it faster and more efficient than using humans. Ticketing for sporting events and concerts has long suffered from the problem of bots continuously checking for inventory then buying any newly released seats to scalp on secondary markets, creating frustrated fans who can't compete with automated technology.

This same behavior is also prevalent in retail e-commerce. Brands like Nike and Supreme continuously release limited edition sneakers. Enthusiasts, known as sneakerheads, take advantage of the hype and deploy bots that jump to the front of the line. Costing only a few hundred dollars, these sneakerbots from websites like hypebots.org, anothernikebot.com, and aiobot.com are used to purchase limited edition sneakers only to resell them at inflated prices elsewhere.

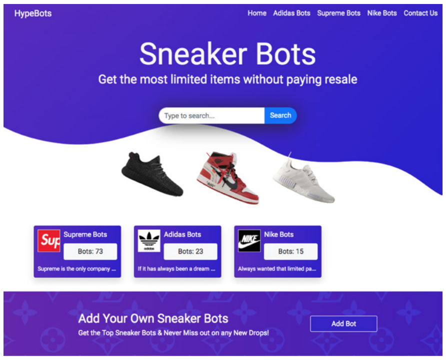
> **"Bots are not benign. They are on websites or mobile apps for a reason, and that reason is to make money."**

Sneaker manufacturers frown on these bots because these customers are not human and don't have a strong, on-going relationship with the brand. More importantly, they don't make additional purchases of other items. Furthermore, after falling for the hype around the new shoes, real customers end up frustrated when they are denied access to the inventory because sneakerbots beat them to the purchase.



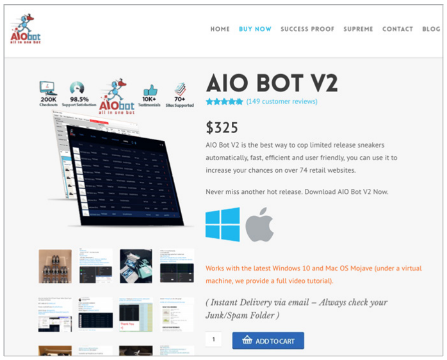
anothernikebot.com

Offers Supreme and Nike bots for sale



hypebots.com

Lists the top 5 bots for purchasing sneakers. Includes Supreme, Nike, and Adidas.



aiobots.com

"The #1 sneaker bot" with testimonials and reviews for $325.

This phenomenon is not limited just to sneakers. During the 2019 Defcon security show, there was a session explaining how to use bots to get your favorite items of clothing called *Rise of the Hypebots: Scripting Streetwear*. Any limited edition or difficult to find item is the target of these hypebots and the game favors those using automation. For bot operators, their business survives on the hype—and using bots.

Bots in the E-commerce Ecosystem

This report is the first industry specific study into the round-the-clock damage caused by bots on e-commerce 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 the business impact is on e-commerce companies.

E-commerce Web Property Structure

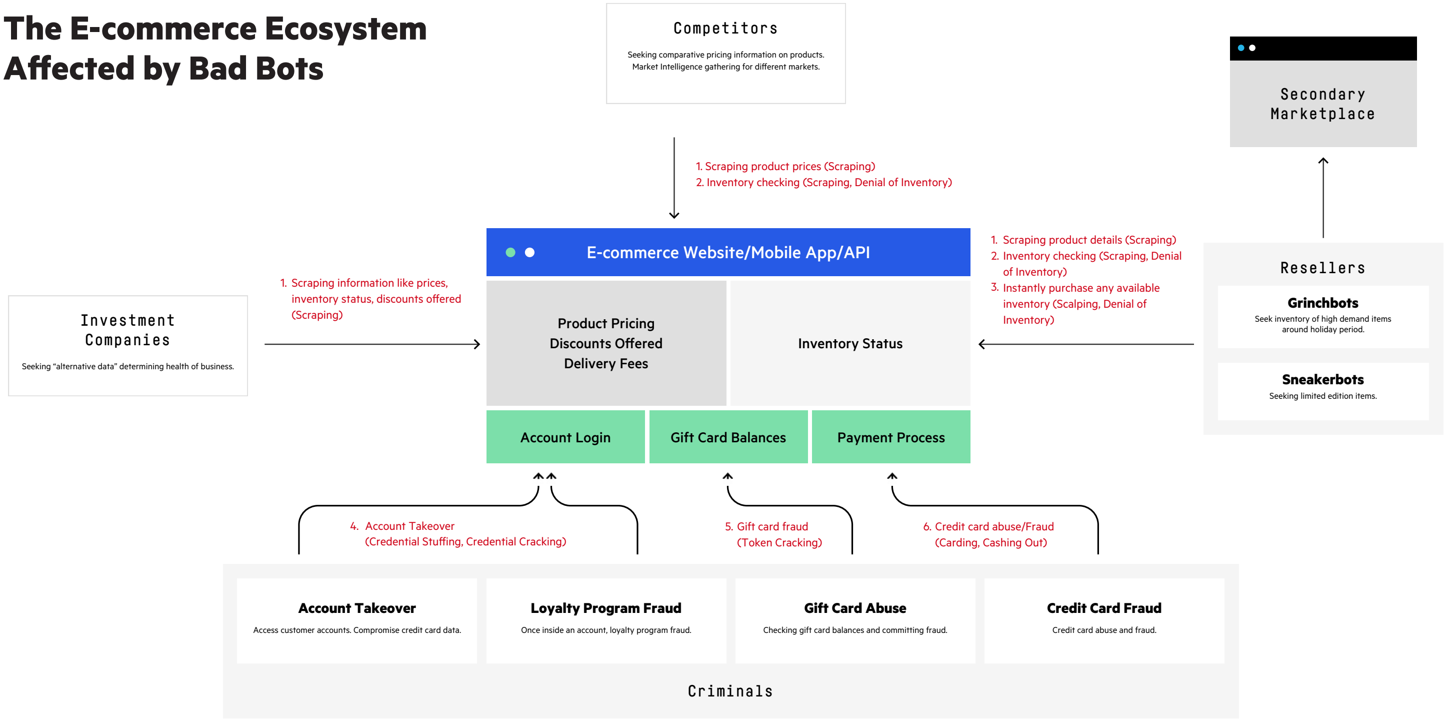
At the heart of the bot problem is the e-commerce website and mobile app. This is the online home for all product information which is presented for customers to make purchase decisions, including pricing, payment processes, gift card functionality, loyalty program details, delivery fees, and more.

For simplicity, e-commerce websites can be thought of as having four distinct areas:

- PRODUCT INFORMATION - Including product features, photos, pricing, discounts, delivery fees, customer reviews, and inventory status.
- CUSTOMER ACCOUNT PAGES - Accessed using credentials and stores purchase records, loyalty program data, personally identifiable information, and any stored payment data.
- GIFT CARD BALANCES - Functionality to understand balances associated with gift cards provided by retailer.
- PAYMENT PROCESSES - Functionality to accept the payment for the products.

Regardless of the specific technical structure of the website, consistent problems plague all e-commerce and online retail platforms in the shape of bots. In general, they are launched from four main groups of bot operators.

The E-commerce Ecosystem Affected by Bad Bots


Competitors
Seeking comparative pricing information on products. Market Intelligence gathering for different markets.
1. Scraping product prices (Scraping)
2. Inventory checking (Scraping, Denial of Inventory)
Secondary Marketplace
E-commerce Website/Mobile App/API
Product Pricing
Discounts Offered
Delivery Fees
Inventory Status
Account Login
Gift Card Balances
Payment Process
Investment Companies
Seeking "alternative data" determining health of business.
1. Scraping information like prices, inventory status, discounts offered (Scraping)
1. Scraping product details (Scraping)
2. Inventory checking (Scraping, Denial of Inventory)
3. Instantly purchase any available inventory (Scalping, Denial of Inventory)
Resellers
Grinchbots
Seek inventory of high demand items around holiday period.
Sneakerbots
Seeking limited edition items.
4. Account Takeover (Credential Stuffing, Credential Cracking)
5. Gift card fraud (Token Cracking)
6. Credit card abuse/Fraud (Carding, Cashing Out)
Account Takeover
Access customer accounts. Compromise credit card data.
Loyalty Program Fraud
Once inside an account, loyalty program fraud.
Gift Card Abuse
Checking gift card balances and committing fraud.
Credit Card Fraud
Credit card abuse and fraud.
Criminals

Bot Operators: Competitors

The web scraping of content by competitors is a major problem for e-commerce companies. Exploiting scraped content is a consistent source of competitive advantage for companies that deploy bots. More specifically, the major goal of competitive scrapers is to gather up-to-date pricing for every product. By being able to dynamically change pricing, particularly on commoditized products, technologically savvy competitors win the SEO battle and steal market share.

Wider market intelligence is also gathered using content scraping bots. If a company is looking to expand into other markets or geographies, bots are deployed to determine what is being sold, and at what price, by the competition. In extreme cases, entire websites are scraped, copied and rebranded for use in other countries.

"Web scraping of content by competitors is a major problem for e-commerce companies."

Bot Operators: Resellers

Resellers actively use automation on e-commerce websites and mobile apps in the form of Grinchbots and Sneakerbots. The appropriately named Grinchbots are deployed seeking inventory of high demand items around traditional holiday periods and cyber week. Resellers anticipate which products will be 'hot items' demanded by children and use bots to hoard as much inventory as possible. This lack of availability creates a secondary market where the 'hot item' is sold at premium prices. Sneakerbots are similar in that they grab as much inventory as possible but they are focused on limited edition or rare items like sneakers made by brands like Nike and Adidas. Again the secondary market is where resellers exploit the demand by customers and charge premium prices for the limited edition items.

Bot Operators: Investment Companies

The financial investment sector also deploys bots to scrape e-commerce companies for information such as pricing data and inventory levels. Sometimes known as alternative data, this information is used by hedge funds to evaluate the health of the e-commerce company to make investment decisions. A recent report estimated that 5 percent of all web traffic is attributable to investment-scraping bots.[4]

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

Bot Operators: Criminals

Criminals exploit the functionality available on e-commerce websites and mobile apps in a variety of ways. Primarily, criminals launch bots aimed at compromising customer accounts. Bots are used in brute force credential stuffing and credential cracking attacks with the goal of gaining access to any customer account. By running stolen credentials against the login pages of e-commerce site, bots identify those accounts where access was granted. Furthermore, once inside an account any stored credit card and personal information could be stolen or used to commit fraud.

The widespread adoption of loyalty programs amongst e-commerce businesses has increased the options for bots to commit fraud. Once inside the customer account, any loyalty rewards can be fraudulently used by the bot operator.

Unique to e-commerce businesses is gift card fraud. Bots are used to exploit the gift card balance checking functionality on a website and enumerate through the multitude of potential combinations of numbers/letters to determine if any contain a remaining balance. Once a gift card number is validated as holding a balance that number can be fraudulently used.

Abuse of the payment process is another bot problem. Specifically, credit card fraud through card cracking is performed by bots.

Spam comments are also posted by bots into product review sections. These posts include links to sites designed to deliver malware to any unsuspecting user.

Account takeover and gift card abuse shakes the confidence of the customer so much that many will no longer use the e-commerce site. Once a customer has been locked out of their account by a criminal changing their password, the e-commerce 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 fraud.

“Criminals launch bots aimed at compromising customer accounts.”

How Bots Affect E-commerce

E-commerce companies are in a continuous and varied war against bad bots. There are consistent business problems created that are caused by the continual barrage of bots. These include unauthorized price scraping, inventory checking, denial of inventory, scalping, customer account takeover, gift card abuse, spam comments, and transaction fraud. Each of these problems alone is enough to have a significant impact on the customer experience and ultimately the reputation of the e-commerce business. 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.

Competitive Price Scraping Affects Revenue

While the specific financial impact of competitors scraping prices is difficult to quantify, it affects revenue, market share, and the overall success of the business. With competitive bots continuously scraping the prices of each product every day, it is difficult to offer discounts or promotions without a competitor matching or beating them instantly. And on the flip side, how do you maintain comparative pricing if you do not know what your competitors are charging for each product? In e-commerce, pricing moves as quickly as the speed of technology.

Information Scraping Bots Affect Share Price

Every e-commerce company knows that in order to maintain website uptime they must deploy additional infrastructure to handle bot and human traffic. The harsh reality is that each company must pay to host unwanted bad bots. To add insult to injury, allowing unfettered access to web scraping bots from investment companies not only requires more bandwidth to support, but can also result in share price fluctuations or difficulty raising capital from the financial markets. Public websites provide valuable data to investment companies looking at the health of the organization and bots are the preferred tool.

> **"The harsh reality is that each company must pay to host unwanted bad bots."**

Duplicate Website Content Affects SEO

Scraped content and websites can appear in other markets in other parts of the world and ultimately have an impact on the SEO rankings of the e-commerce website. In the highly competitive e-commerce space, a website with higher search engine rankings earns more attention and ultimately more revenue.

Denial of Inventory & Scalping: Creating the Reseller Market

Sneakerbots and Grinchbots, by continuously checking for inventory of limited edition items, and immediately purchasing any that are available not only block real customers from purchasing the product, they also help create the secondary market. An anxious parent looking to purchase a toy grabbed by an unscrupulous Grinchbot will quickly turn to reseller marketplaces and have their frustration heightened when they see the item listed for a premium price considerably higher than on the original website. While the e-commerce website made the sale of the item, the lifetime value of the Ginchbot is not as valuable as a satisfied customer who regularly returns to buy additional products. The lost sale leads to potential brand damage because the frustrated human associates the e-commerce website as making false claims and not having enough inventory. In the frustrated customer's eyes, the fault lies with the e-commerce company not the Grinchbot.

Accessing Customer Accounts Causes Brand Damage

Criminals use bots to perform account takeover of customer accounts. Once inside the account, any loyalty rewards can be used. 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. An increase in complaints about loss of loyalty points is another indicator of increased bot activity resulting from account takeover. Customer's locked out of an account are less likely to use the website ever again and the brand damage of an account takeover in many cases results in a lost customer.

"Gift card fraud abuse leads to angry customers when they notice that balances have disappeared."

Gift Card Fraud Costs Are High

Gift card fraud abuse leads to angry customers when they notice that balances have disappeared. The forensic costs to investigate the incident and reimburse the gift card balance are significant, as are the chances of retaining that angry customer.

Fraud: A Cost of Doing Business?

Credit card fraud is a constant problem for any e-commerce business. 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. On the positive side, reducing the total volume of bot traffic on the website or mobile app typically lowers the amount of attempted automated fraud during transactions.

Higher Infrastructure Costs

Bots skew the analytics gathered from the website and adversely affect conversion rates. This volume of bots on e-commerce sites is significant and continuous. The business must spend money on additional infrastructure to make sure their website doesn't suffer from brownouts or downtime.

The Equation of How Bots Affect E-commerce

A summary of business problems that are caused by bots is shown below.

BOT ACTIVITY	E-COMMERCE IMPACT
1 **Scraping Prices and Content**	Allows competitors ability to change prices quickly. Minimizes success of discounts or promotions. Loss of market share to lower priced competitors. Investment community evaluates the health of the business. Share price affected. Difficulty in raising finance from investment community. Duplicate content appears elsewhere and damages SEO.
+	
2 **Denial of Inventory**	Real customers unable to buy product at retail price. Helps create the secondary market. Customer frustration and retention problems. Brand damage.
+	
3 **Scalping by Resellers**	Real customers unable to buy product at retail price. Customers pay premiums over retail price on secondary reseller marketplaces. Customer frustration and retention problems. Brand damage.
+	
4 **Customer Account Takeover**	Angry customers, higher customer service costs. Forensic investigations, reimbursement costs. Customer retention problems. Increased loyalty program fraud. Brand damage.
+	
5 **Credit Card Fraud**	Angry customers, higher customer service costs. Forensic investigations, reimbursement costs. Customer retention problems. Brand damage.
+	
6 **Gift Card Fraud**	Angry customers, higher customer service costs. Forensic investigations, reimbursement costs. Customer retention problems. Brand damage.
=	
7 **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 e-commerce 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.

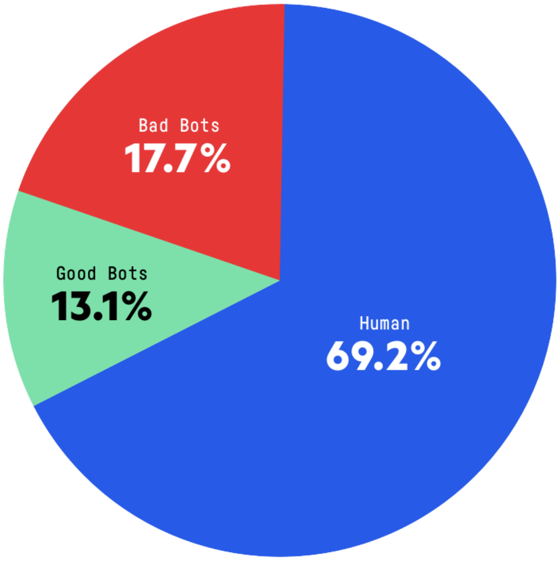
NUMBER OF DOMAINS	231
TIME PERIOD	24 Days
DATE OF DATA GATHERING	July 2019
NUMBER OF REQUESTS	16.4 billion

The Bots on E-commerce Platforms

On e-commerce websites and mobile apps bots comprise 30.8 percent of traffic. As you would expect with retailers selling consumer products there are a significant volume of humans at 69.2 percent of all traffic.

Bad bots that perform scraping, account takeover, gift card abuse, credit card fraud and reseller inventory denial know what they are after trying to exploit and comprise 17.7 percent of all traffic.

Bad Bot vs. Good Bot vs. Human E-commerce



How Bad is Bad?

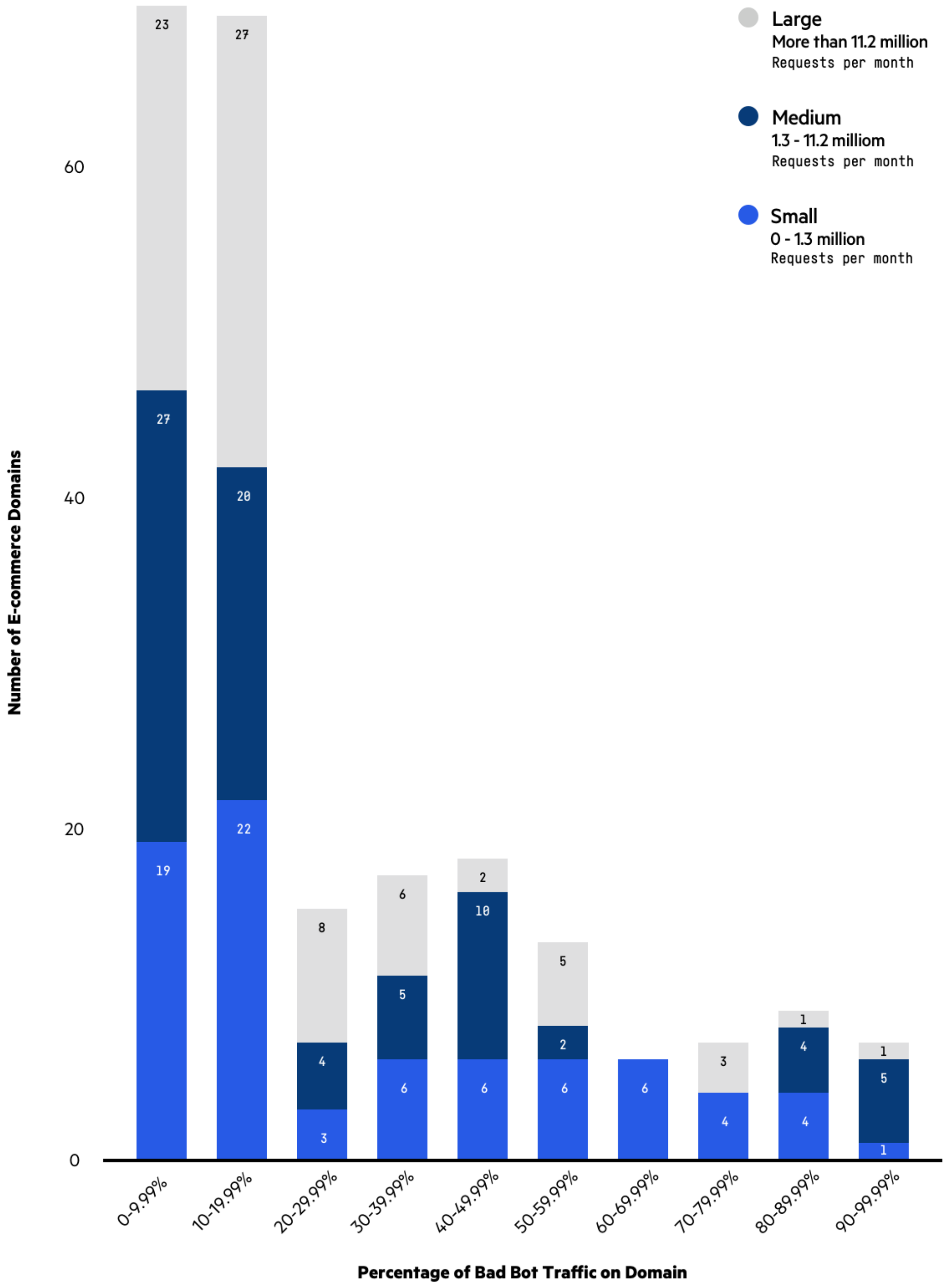
While the average bad bot traffic across 231 domains was 17.7 percent, this aggregate doesn't tell the full story. Some domains receive considerably higher proportions of bad bot traffic. The variances by domain and by page within a domain are extreme. Bots know what they are seeking and are focused on the goal of the bot operator. It really does depend on the website's functionality and the data it contains. No two bot problems are identical.

As illustration, the domain identified as suffering from the highest proportion of bot traffic was a medium sized European site—99.15 percent of its traffic was bad bots. Humans accounted for only 0.34 percent of its traffic.

Finally, across all industries the amount of bad bots seen is 20.4 percent[5]. In this study, 90 e-commerce domains exceed this proportion of bad bot traffic. And on 77 of the domains in the study, bad bots accounted for greater than 30 percent of all traffic.

[5] 2019 Bad Bot Report: The Bot Arms Race Continues

Number of E-commerce Domains by Percentage of Bad Bot Traffic



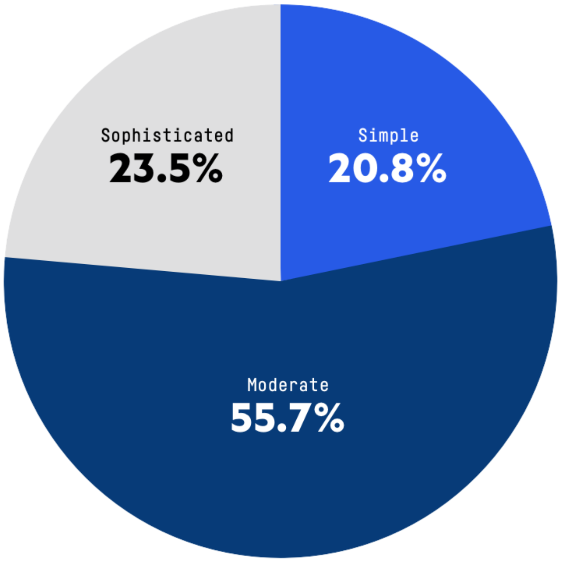
E-commerce Bot Sophistication Rises

Nearly a quarter (23.5 percent) of bots on e-commerce domains were classified as sophisticated. Only 20.8 percent were simple bots. The remaining 55.7 percent were moderately sophisticated.

Echoing trends seen in other industries, the sophistication level of bots on e-commerce platforms is rising higher than previously seen in the 2019 Bad Bot Report. In that research, 21.4 percent of bots on e-commerce were sophisticated compared with 23.5 percent now.

The proportion of simple bots is dropping while there has been a slight increase in the percentage of moderate bots seen on e-commerce platforms. This increasing sophistication is explained by the arms race at play between bot operators and bot detection technology tools. 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 competitors and resellers is based upon bots scraping data, the cycle continues ad infinitum.

Sophistication of Bots - E-commerce



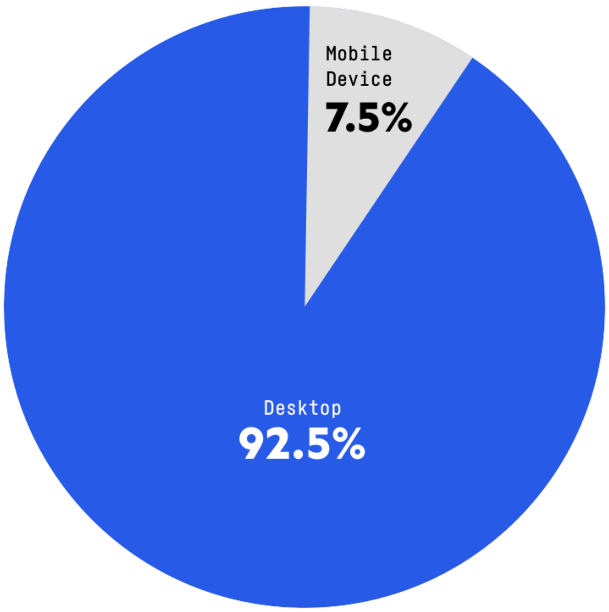
BOT SOPHISTICATION	E-COMMERCE DOMAINS 2018[6]	E-COMMERCE DOMAINS 2019
Sophisticated	21.4%	23.5%
Moderate	54.4%	55.7%
Simple	24.2%	20.8%

[6] 2019 Bad Bot Report: The Bot Arms Race Continues

Mobile versus Desktop Bots

While 7.5 percent of bots identify as user agents from mobile devices in e-commerce, compared with other industries like ticketing or airlines, less bad bots identify as originating from a mobile device. The rest (92.5 percent) all claim a user agent associated with a desktop browser.

Bad Bot User Agent Type

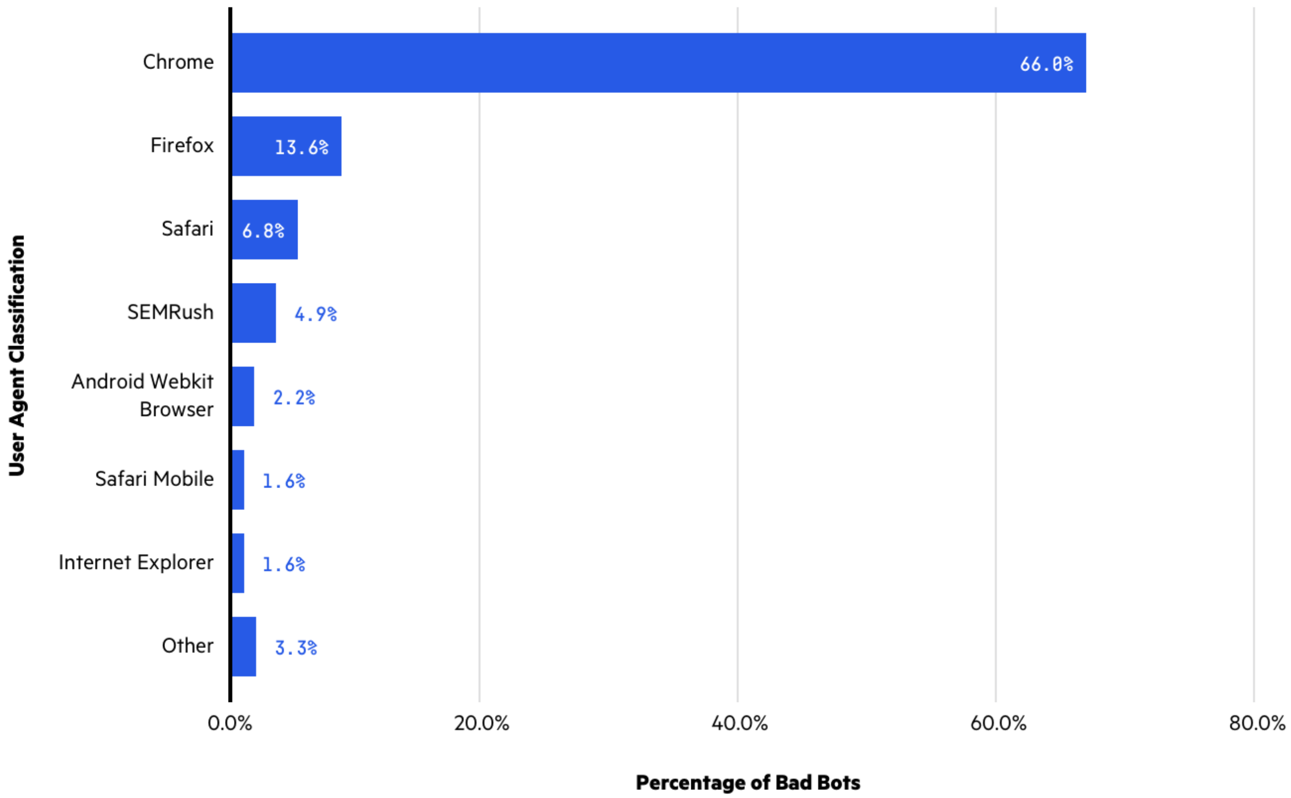


Top Self Reporting Browsers

Across all e-commerce domains, bad bots identified themselves as one of 435 unique user agents. A far higher proportion of bad bot traffic in this industry identify as Chrome with 66.0 percent of all bots claiming that identity. Comparing all other industries, just under half (49.9 percent) of all bots identify as Chrome[7.] Clearly more e-commerce bots are attempting to hide in plain sight by impersonating the most popular browser.

Firefox is the next most popular identity for bad bots but at a distant 13.6 percent, followed by Safari at 6.8 percent. Unique to e-commerce, 4.9 percent of bad bots are identifying as SEMRush, a tool used to provide online analytics. The leading mobile user agents claimed by bad bots were Android Webkit Browser (2.2 percent) and Safari mobile with 1.6 percent.

Bad Bot Reported User Agent Types on E-commerce Domains



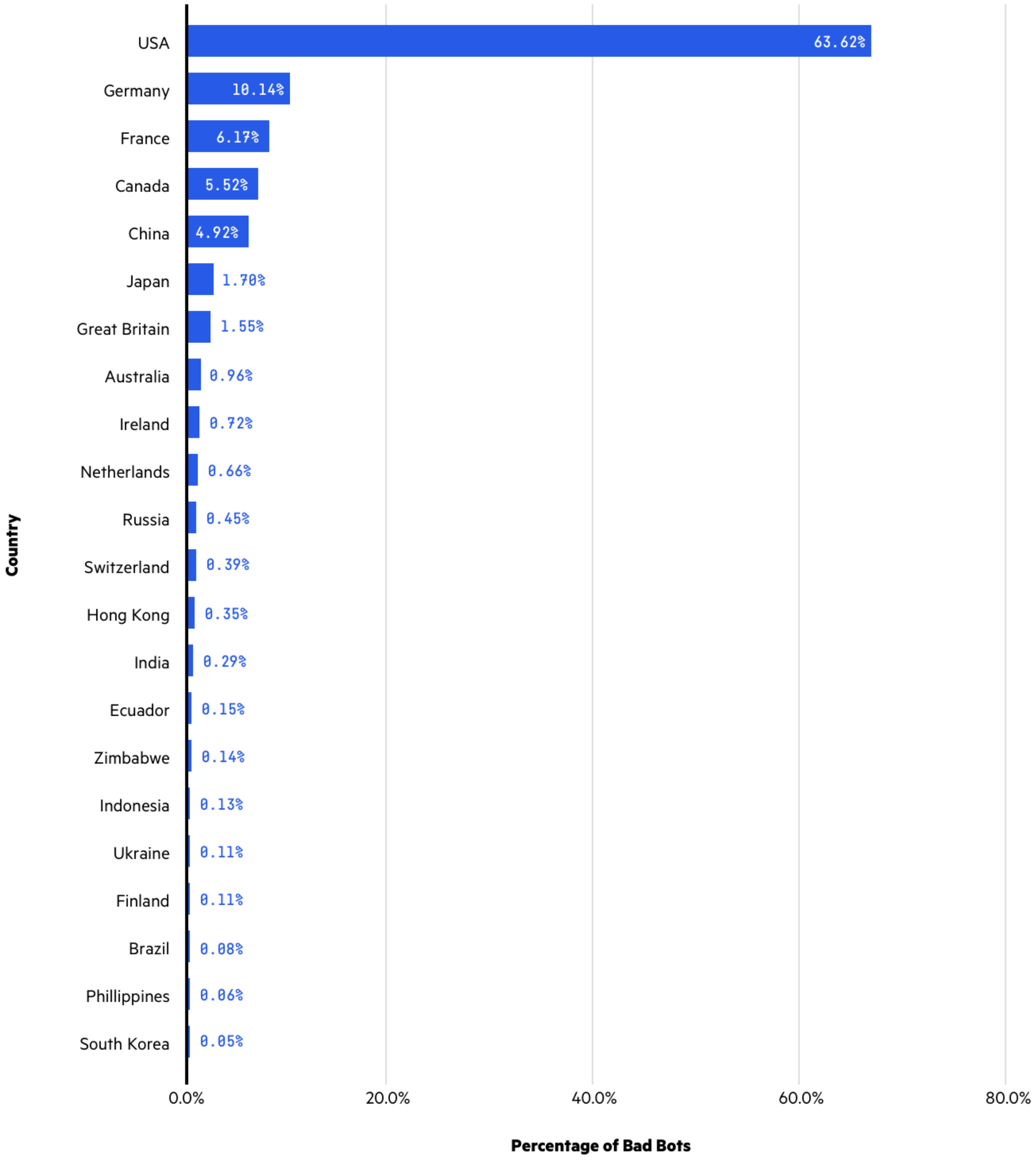
[7] 2019 Bad Bot Report: The Bot Arms Race Continues

Bad Bots Originated from the USA

USA is the leading source of bad bots on e-commerce websites and mobile apps and is responsible for 63.62 percent of this traffic. This proportion is higher than the contribution the USA makes for all industries—in the 2019 Bad Bot Report, USA was responsible for 53.4 percent of all bad bot traffic.

Germany is in second place and is responsible for 10.14 percent of bad bot traffic. France (6.17 percent), Canada (5.52 percent) and China (4.92 percent) round out the top five and each country contributes a higher proportion of bad bot traffic on e-commerce sites compared to other industries.

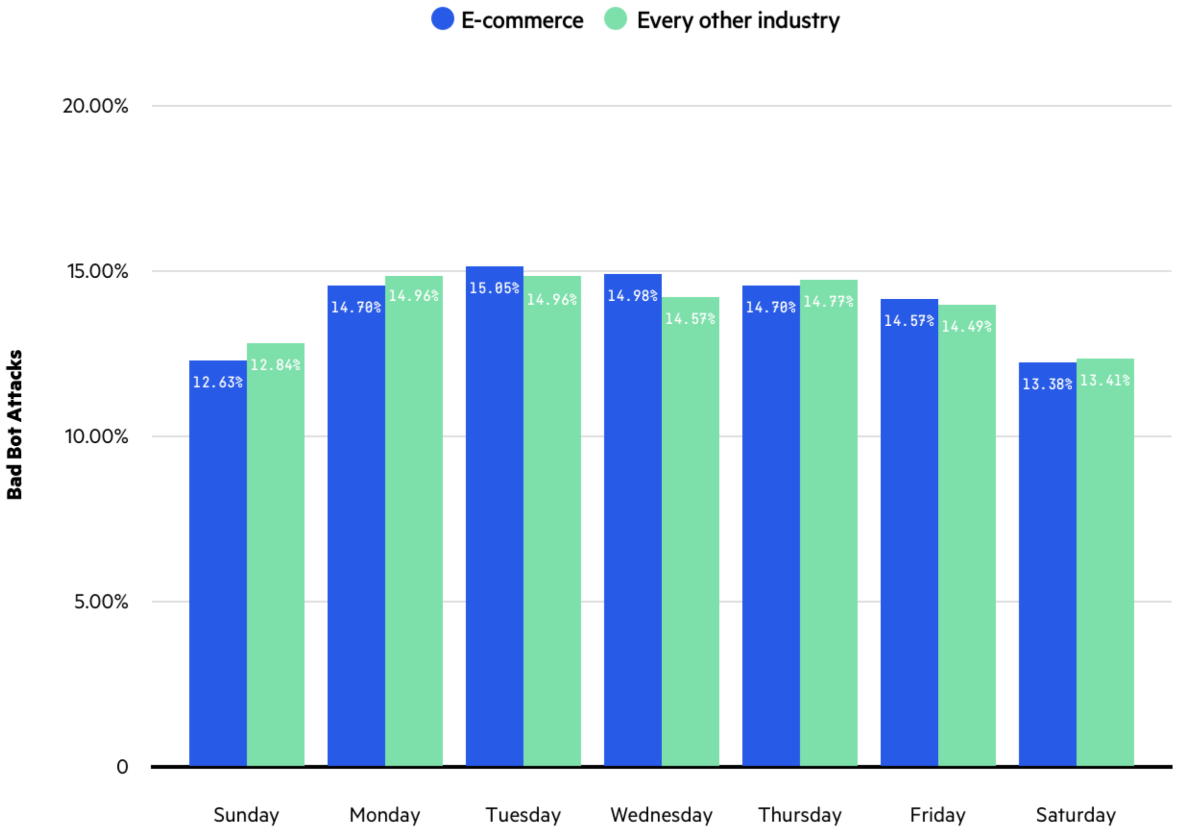
Bad Bot Originating Countries on E-commerce Domains



E-commerce Bots By Day of the Week

Similar to the results seen for other industries, the consistency of bad bot traffic on e-commerce 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. Saturday and Sunday are the days with the lowest amount of bad bot traffic indicating that bad bot operators are not as active on the weekends again highlighting that running bots is a day job.

Bad Bot Attack Distribution by Day of the Week
E-commerce and Every Other Industry



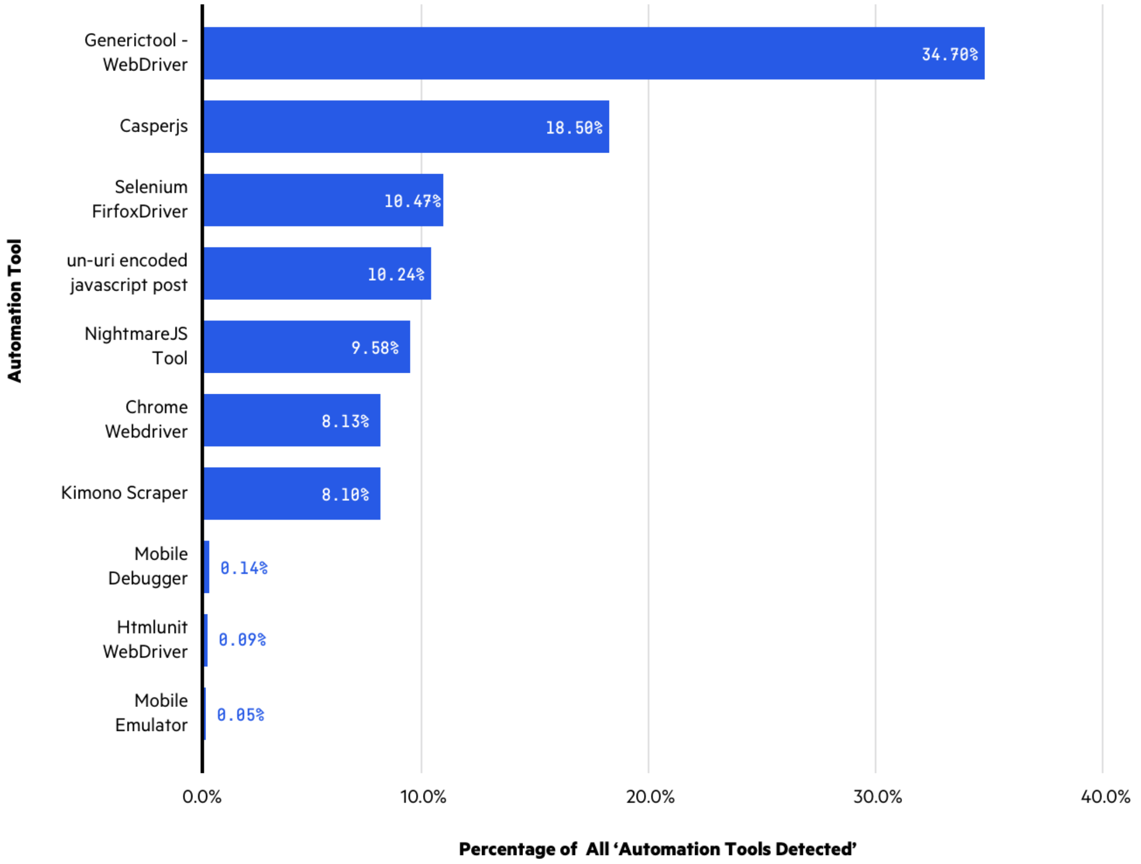
Popular Automated Tools Used on E-commerce Domains

Of the bad bots identified as an “Automated Tool”, a generic automation framework (WebDriver) was the most popular accounting for 34.7 percent of those detected. Casperjs (18.50 percent) was the second most popular tool detected on e-commerce domains.

Different versions of Selenium also saw significant usage—Selenium “Firefox” with 10.47 percent and Selenium “Chrome” with 8.13 percent.

Mobile tools were also detected but at a much lower rate than on other industries like ticketing. Mobile debugger’s accounted for only 0.14 percent of automated tools and mobile emulators were less at 0.05 percent, which further indicates the mobile bots are not as popular in e-commerce as they are in other industries.

Most Popular Automated Tools Detected on E-commerce Domains



Bots Perform Account Takeover

Bots run credential cracking and credential stuffing attacks to identify which pairs of usernames and passwords provide 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 to the demands placed on the backend database during repeated authentication attempts.

The typical range of volumetric account takeover attacks is 2-3 per month[8].

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.

[8] Research Lab: The Anatomy of Account Takeover Attacks

Recommendations

Bots are on e-commerce 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 CAPTURE 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 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
- GigeNET
- 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.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.

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. Your defenses need to evolve as fast as the threats, and to do that you need dedicated support from a team of experts.

About Imperva Bot Management

In July 2019, Imperva acquired Distil Networks, the global leader in bot mitigation that 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. Imperva Bot Management is the new product name.

About Imperva Application Security

Imperva Application Security mitigates risk for your business with full-function defense-in-depth, providing protection wherever you choose to deploy - in the cloud, on-premises, or via a hybrid model. Imperva offers advanced analytics to quickly identify the threats that matter, Web Application Firewall (WAF) solutions which block the most critical web application security risks, DDoS protection with a 3-second mitigation SLA, API Security that integrates with leading API management vendors, Bot Management for protection against all OWASP automated threats, Runtime Application Self-Protection (RASP) for security by default against known and zero-day vulnerabilities, and a developer-friendly Content Delivery Network (CDN) for the utmost performance. Through FlexProtect, our unique licensing model, you can deploy Imperva Application Security how and when you need it. FlexProtect helps protect your applications wherever they live — in the cloud, on-premises or in a hybrid configuration.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com

imperva