radware | SHIELDSQUARE

Radware-ShieldSquare Research

THE E-COMMERCE INDUSTRY AUTOMATED THREAT LANDSCAPE

A Recap of Bad Bot Trends in 2019

DECEMBER 2019

Table of Contents

E-commerce firms across the globe are searching for more efficient ways to connect with customers and retain existing ones. Secure and easy-to-use applications are critical to success in rapidly changing market conditions. However, e-commerce firms have lately reported growing bad bot attacks on their web applications, mobile apps, and APIs.

To understand how cybercriminals are targeting e-commerce firms, ShieldSquare studied the traffic of e-commerce firms from its global client base during Q1 – Q3, 2019. What follows is an in-depth analysis of different types of attacks that e-commerce firms are facing from bots including highlights on 2019 Black Friday and Cyber Monday.

The report also highlights a type of bad bot discovered by security researchers from ShieldSquare. Dubbed "AuthBot", this new botnet is targeting e-commerce firms with account takeover attacks to steal PII and payment card details.

Executive Summary

The E-commerce industry is growing fast. In a matter of seconds, lucrative shopping deals are being availed and transactions are done. If an organization's IT infrastructure is not up to the task of protecting applications that enable easy shopping, sophisticated automated attacks can happen in the blink of an eye.

The sophistication level of bad bots is increasing across the industries. Their ability to mimic human behavior and be distributed over thousands of IPs is a major cause of concern to e-commerce firms and their applications. The fourth-generation bad bots are not only capable of mimicking human behavior, but they can also be distributed over thousands of IPs and can automatically mutate to carry out cyber-attacks. Cybercrime group behind AuthBots (refer Section 1: The AuthBot Operation to learn more) is also leveraging fourth-generation bad bots to perform account takeover attacks.

eCommerce businesses rely on 'good bots' to promote their business. Bots provides them more visibility in the virtual space, whether by digital advertising, search engines, social networks and affiliate programs. Therefore, these bots play a key role in online shopping and should be let through. However, as 'bad' bots carryout cyberattacks, the precision in classification is crucial and has an immediate business impact (ROI).

To better understand the threats that e-commerce firms are facing from bad bots, ShieldSquare (a part of Radware) commissioned a research to study the traffic of e-commerce businesses to understand characteristics of attacks that e-commerce firms are facing, bad bots' behavior during big shopping days such as Black Friday and Cyber Monday, and the rise of AuthBots. The report answers the following questions in detail:

- What is AuthBot and why e-commerce firms should be wary of it
- How bad bots targeted e-commerce firms during Black Friday and Cyber Monday
- What are the distribution of internet traffic among (1) Good Bots (2) Bad Bots (3) Humans
- What are the most targeted industries by bad bots?
- What types of bots target e-commerce businesses?
- What are four major threats to e-commerce firms from bad bots

KEY FINDINGS

- 26.4% of the traffic on e-commerce sites was bad bot during Q1 – Q3, 2019.
- On Black Friday, 38.6% and on Cyber Monday, 42.5% of traffic was bad bots on e-commerce firms.
- A new type of bot, dubbed "AuthBot", is targeting login pages of e-commerce firms. AuthBots made 2.3 billion hits on the login pages of e-commerce sites during Q1 – Q3, 2019.
- So far in 2019, 56% of bots on e-commerce sites were of high sophistication. These fourth-generation bots can be distributed over thousands of IPs based in different geographical locations and can masquerade as human users.

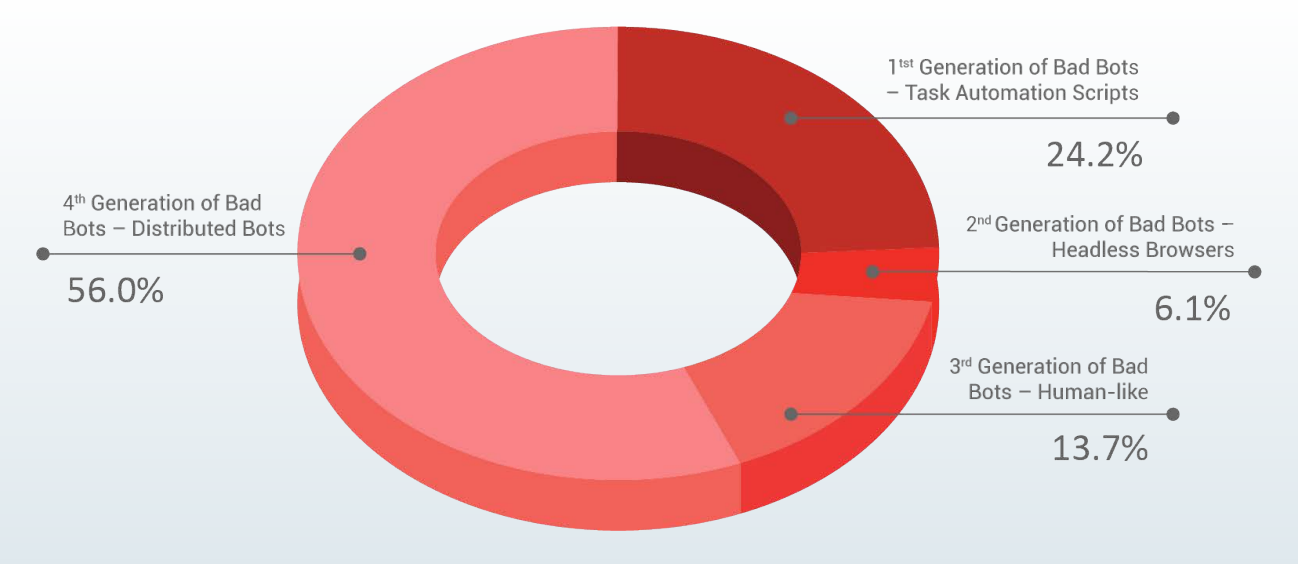


Figure 1: Types of Bots on E-commerce Businesses

Section 1: The AuthBot Operation

Cybercriminals are siphoning PIIs of millions of shoppers. Dubbed "AuthBot" because of their persistent attempts at cracking authentication, this botnet group targets e-commerce firms with large-scale credential stuffing & cracking attacks to take over user accounts. Using an army of bots run from fraudulently acquired IP addresses, the AuthBots made nearly 100 million hits on login pages of e-commerce businesses during Q1 – Q3 2019. All e-commerce firms with mandatory login are targeted by AuthBots.

Our security researchers first noticed similar bot fingerprints across many e-commerce domains in late 2018 and started tracking the botnets. The following report illustrates the sophistication and rapid evolution of AuthBots and its damaging effect on the e-commerce ecosystem. The analysis is possibly only a fraction of AuthBot's true impact. The total ongoing impact of AuthBots on the e-commerce ecosystem may be larger since ShieldSquare researchers' analysis is limited to the domains monitored by us.

A Snapshot of AuthBot Operation

Observed First: Late 2018

VOLUME

NEARLY

2.3

BILLION HITS ON LOGIN PAGES OF E-COMMERCE FIRMS DURING Q1 – Q3 2019

OPERATION INFRASTRUCTURE

52

MILLION OF AUTHBOT HITS ORIGINATED FROM 10 PROMINENT DATA CENTERS/ PUBLIC CLOUDS

Operation method: (1) Credential stuffing attacks using stolen/purchased credentials
(2) Credential cracking or brute force attack

Advanced Techniques to Evade Detection

- Manipulation of geolocation and IP addresses through Proxy Servers
- Most of IPs used by AuthBots are in the US
- Distributed over hundreds of randomly assigned IP addresses & residential proxies
- Human-like keystrokes and mouse movements
- Use of machine learning and Robotic Process Automation (RPA) to help bots work as a standalone software module
- Daisy-chained to manage through one centralized server

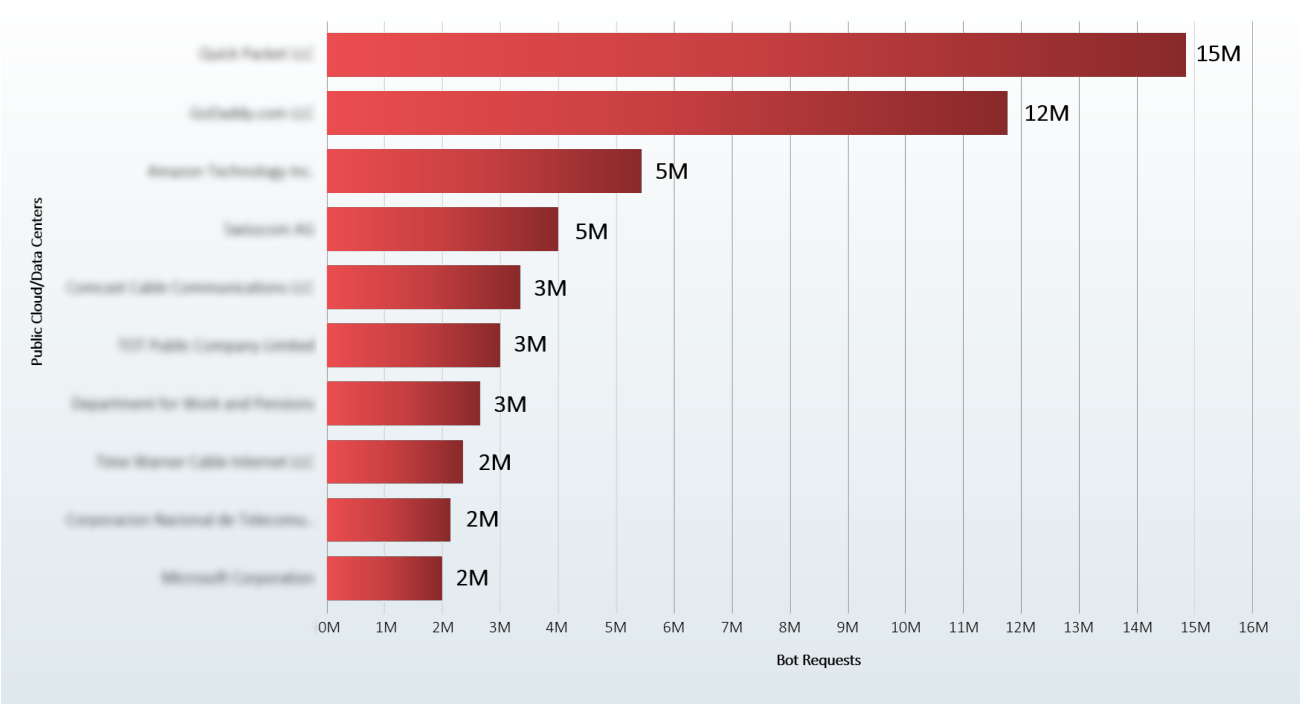


Figure 2: Origin of AuthBots – Top 10 Public Cloud/Data Centers

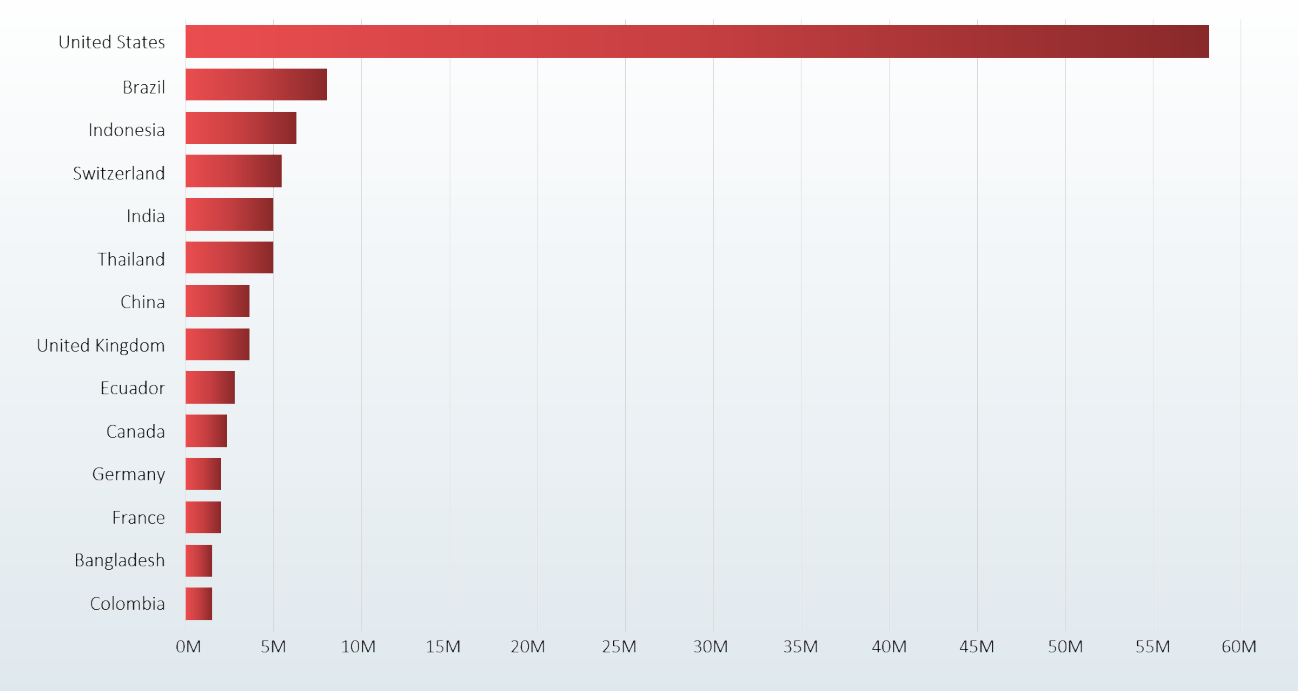
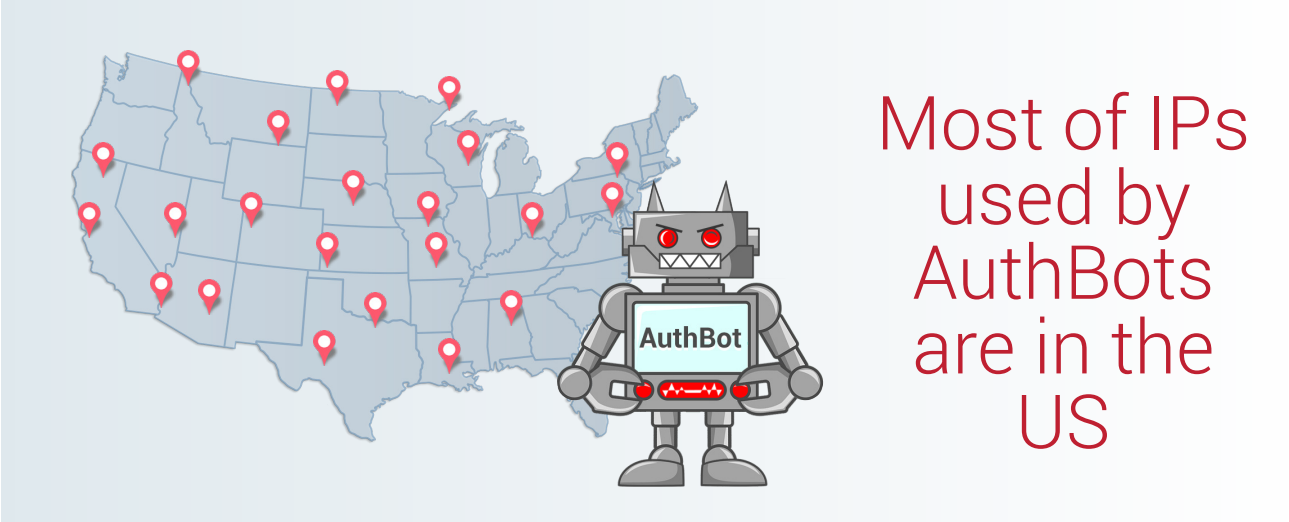


Figure 3: Origin of AuthBots – Top Countries



Business Impact

- From Q1 – Q3 2019, a significant percentage of traffic was AuthBots on targeted e-commerce firms' login page.
- Once an AuthBot operation is successful, PII and payment card details of compromised accounts are stolen.

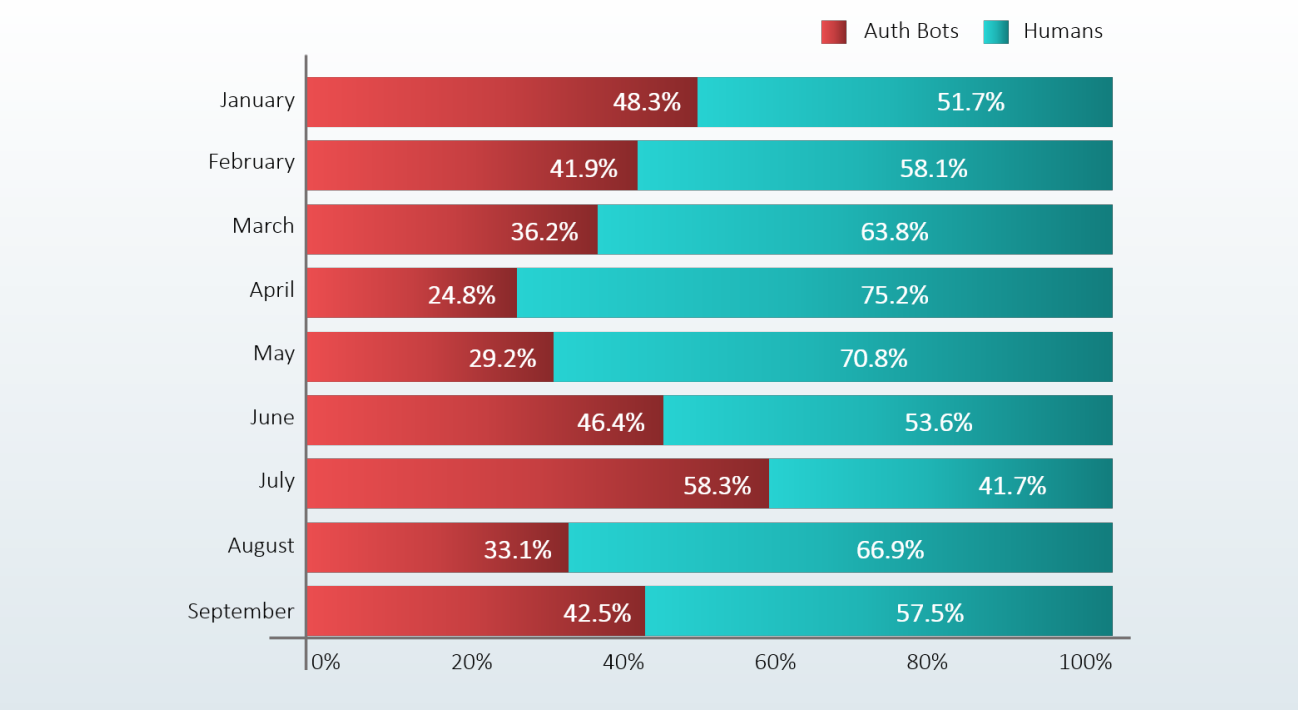


Figure 4: Business Impact of AuthBots – Monthly Presence

Section 2: Black Friday and Cyber Monday 2019

- On Black Friday, 38.6% of traffic was bad bots on e-commerce firms.
- On Cyber Monday, 42.5% of traffic was bad bots on e-commerce firms.
- These bots were observed performing account takeover, denial of inventory, and content scraping attacks among others.

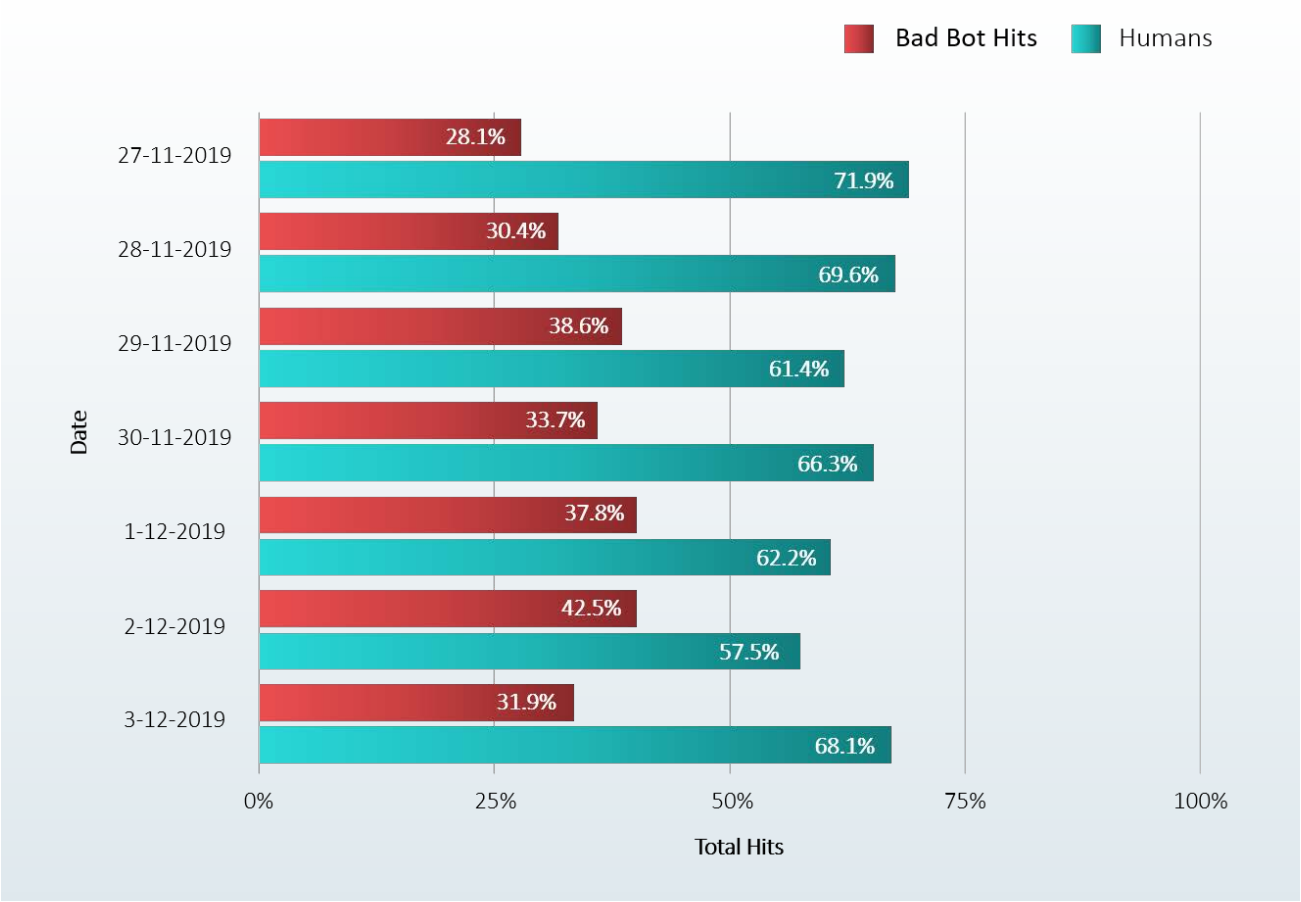


Figure 5: Black Friday and Cyber Monday 2019

Account Takeover Attacks

- Nearly two-thirds of the traffic on the login pages were bots during Black Friday and Cyber Monday. These bots were observed performing account takeover attacks during the shopping days.
- Only one-third of the traffic was human on e-commerce sites during Black Friday and Cyber Monday this year
- Most of these bots were AuthBots and were distributed over thousands of IPs.

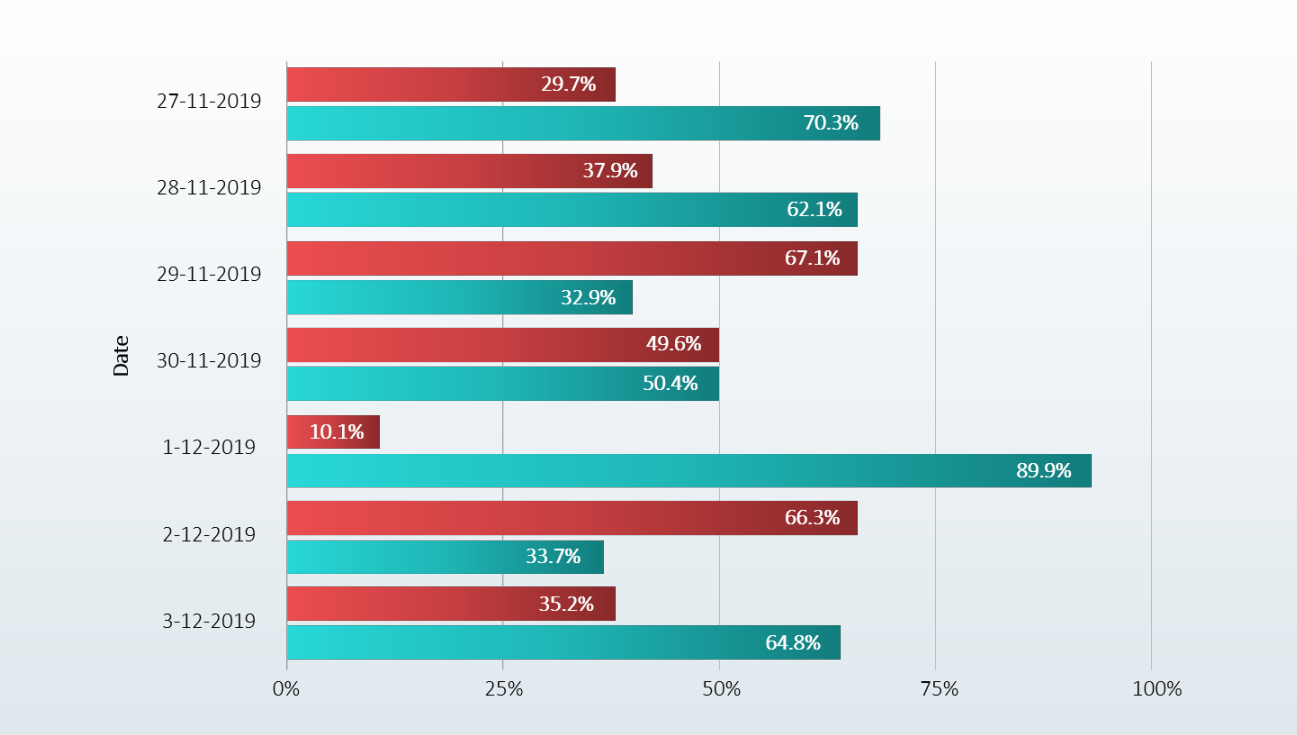


Figure 6: Black Friday and Cyber Monday 2019 – Account Takeover Attacks

Denial of Inventory Attacks

- Nearly 90% of the traffic on the cart page of e-commerce sites during Cyber Monday was bots on a significant number of e-commerce sites monitored by us.
- On Black Friday, nearly two-thirds of the traffic was bots.
- This was the reason behind the higher cart abandonment rate on Black Friday and Cyber Monday.

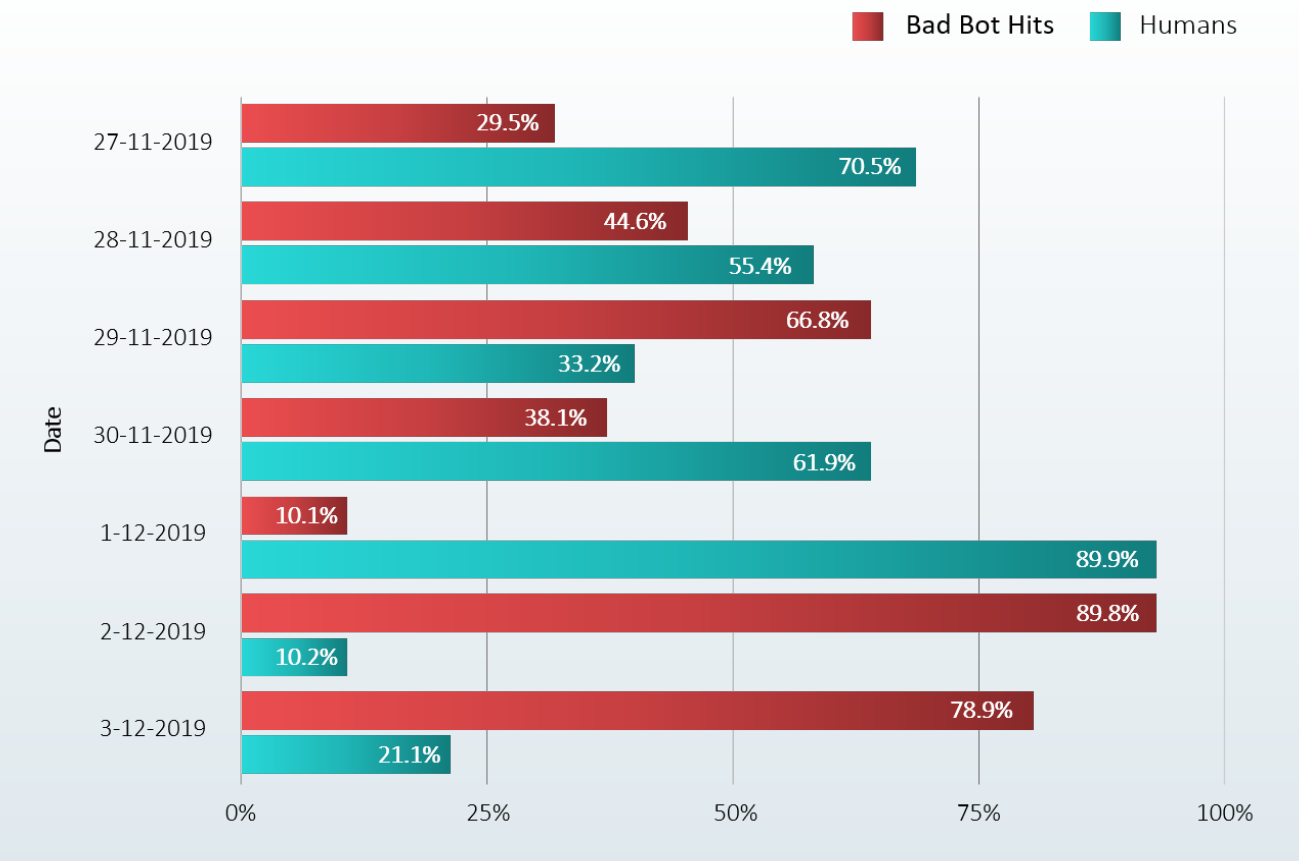


Figure 7: Black Friday and Cyber Monday 2019 – Denial of Inventory Attacks

Content Scraping Attacks

- 40.1% of the traffic of category pages and 45.3% of the traffic on product pages was bots during Black Friday.
- 41.8% of the traffic of category pages and 40.2% of the traffic on product pages was bots during Cyber Monday 2019.
- These bad bots attempted to perform scraping of product listing and details from category and product pages of e-commerce firms.

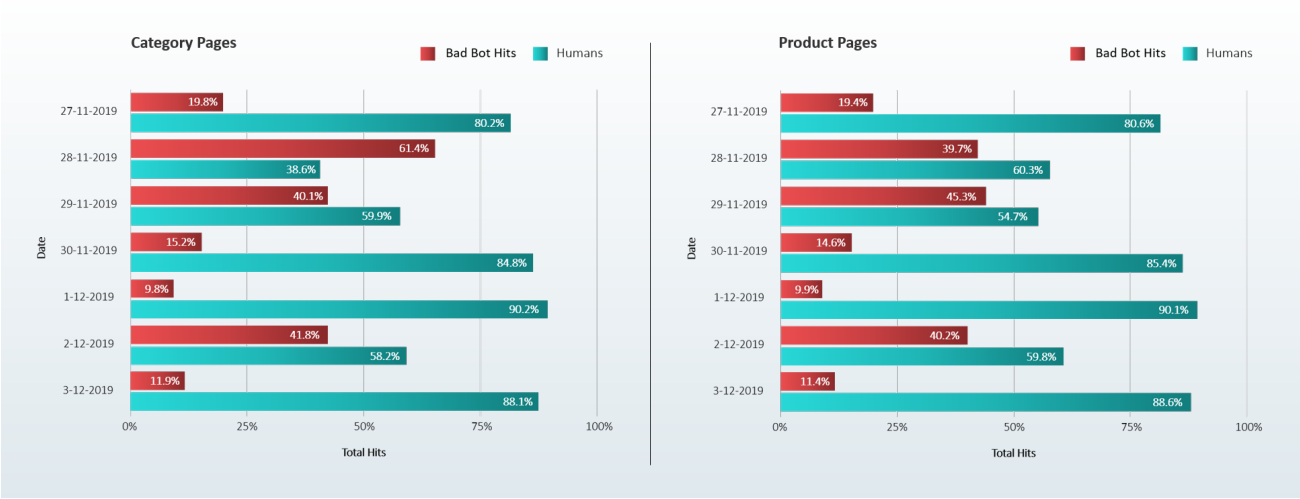
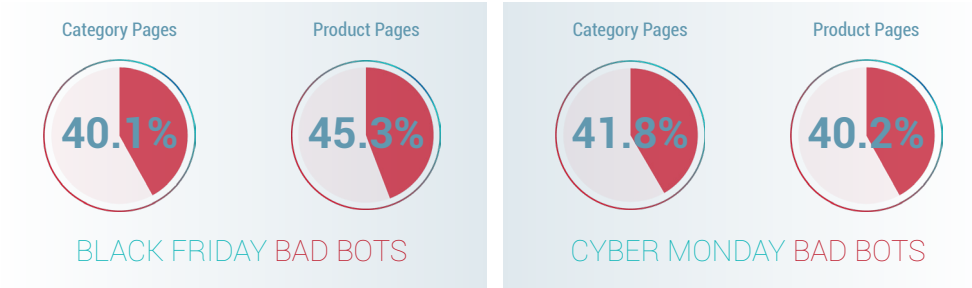


Figure 8: Black Friday and Cyber Monday 2019 – Content Scraping Attacks



Origin of Bad Bots – Black Friday

- Most of the bad bots on Black Friday originated from the US, followed by the UK and Brazil.
- Cybercriminals leverage proxy servers to show their IP locations from countries of business importance.

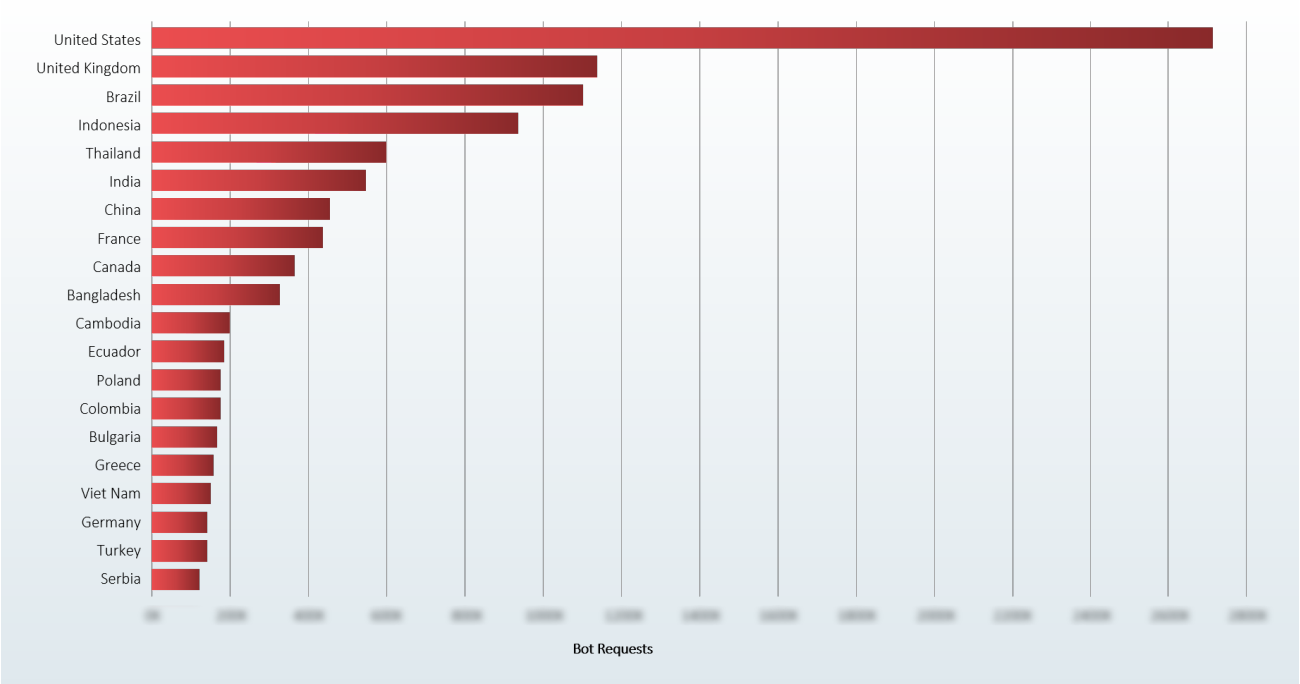


Figure 9: Origin of Bad Bots – Black Friday

Most of the bad bots on Black Friday originated from the US, followed by the UK and Brazil.

Origin of Bad Bots – Cyber Monday

- Most of the bad bots on Black Friday originated from the US, followed by Brazil and Indonesia.
- Cybercriminals leverage proxy servers to show their IP locations from countries of business importance.

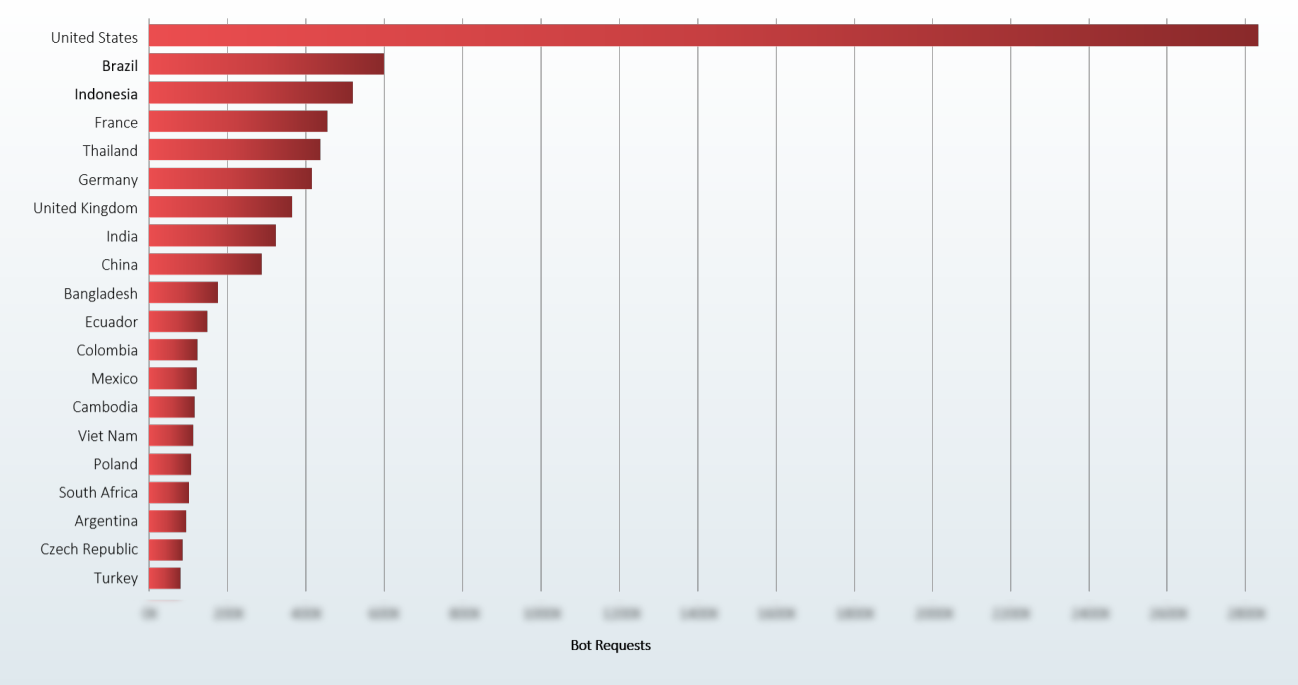


Figure 10: Origin of Bad Bots Cyber Monday

Most of the bad bots on Black Friday originated from the US, followed by Brazil and Indonesia.

Section 3: Industry-Wide Bad Bot Trends

Internet Traffic Distribution

- In first three quarters of 2019, 23.9% of traffic was bad bots
- 49.3% of total traffic was bots in the first three quarters of 2019.

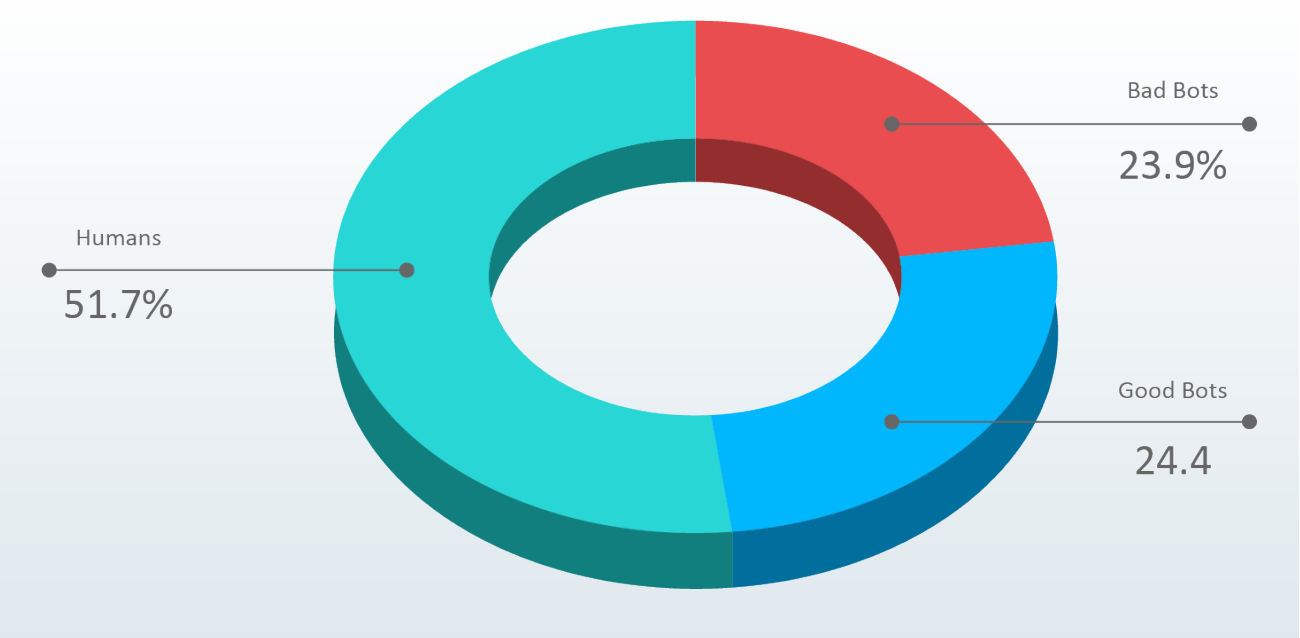


Figure 11: Internet Traffic Distribution

Most Targeted Industries by Bad Bots

- With 26.4% of the traffic as bad bots, the e-commerce industry was the most targeted industry in the first three quarters of 2019, followed by real estate, online marketplaces and classifieds, and digital publishers.

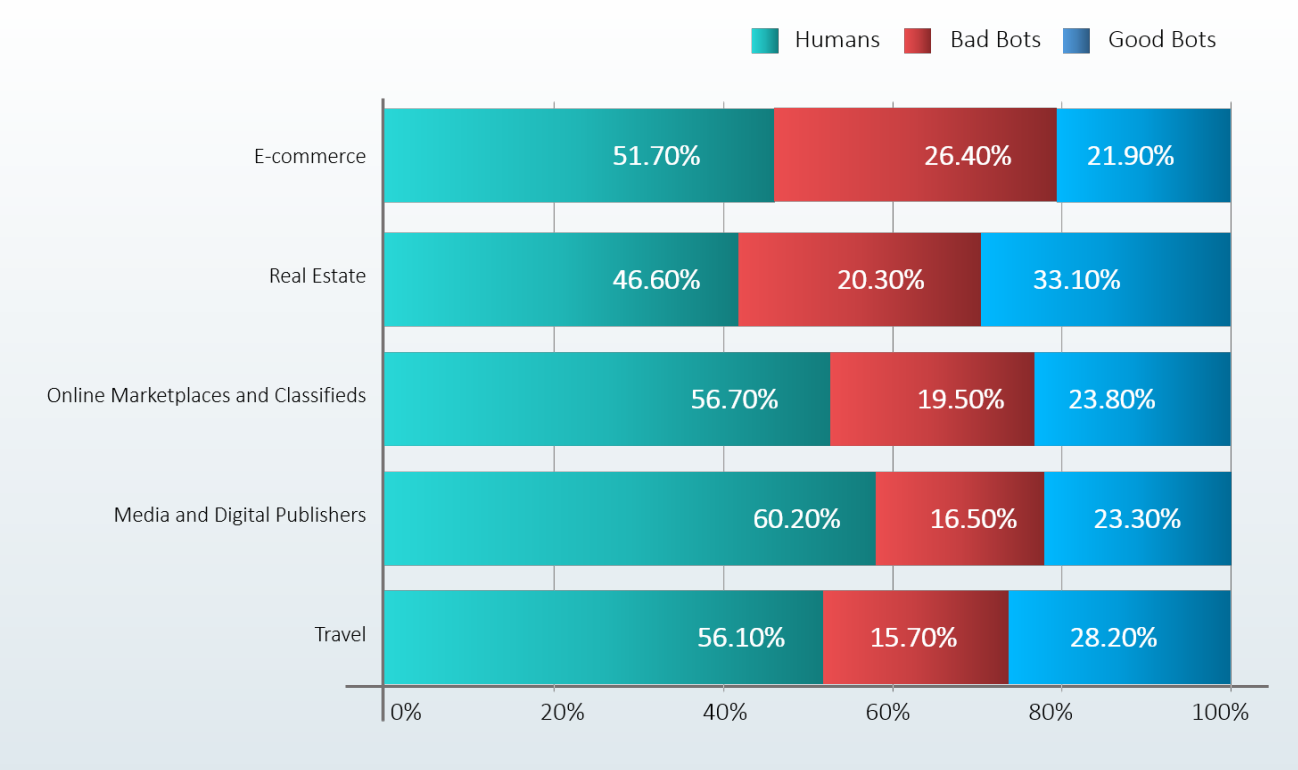


Figure 12: Most Targeted Industries by Bad Bots

Section 4: E-commerce Industry Automated Threat Landscape

Origin of Bad Bots Targeting E-commerce Industry

- Most of the bad bots originated from the US, followed by Italy, Germany, and China.
- Bots leverage proxy servers to show their IP addresses from countries of business importance to avoid being blocked.

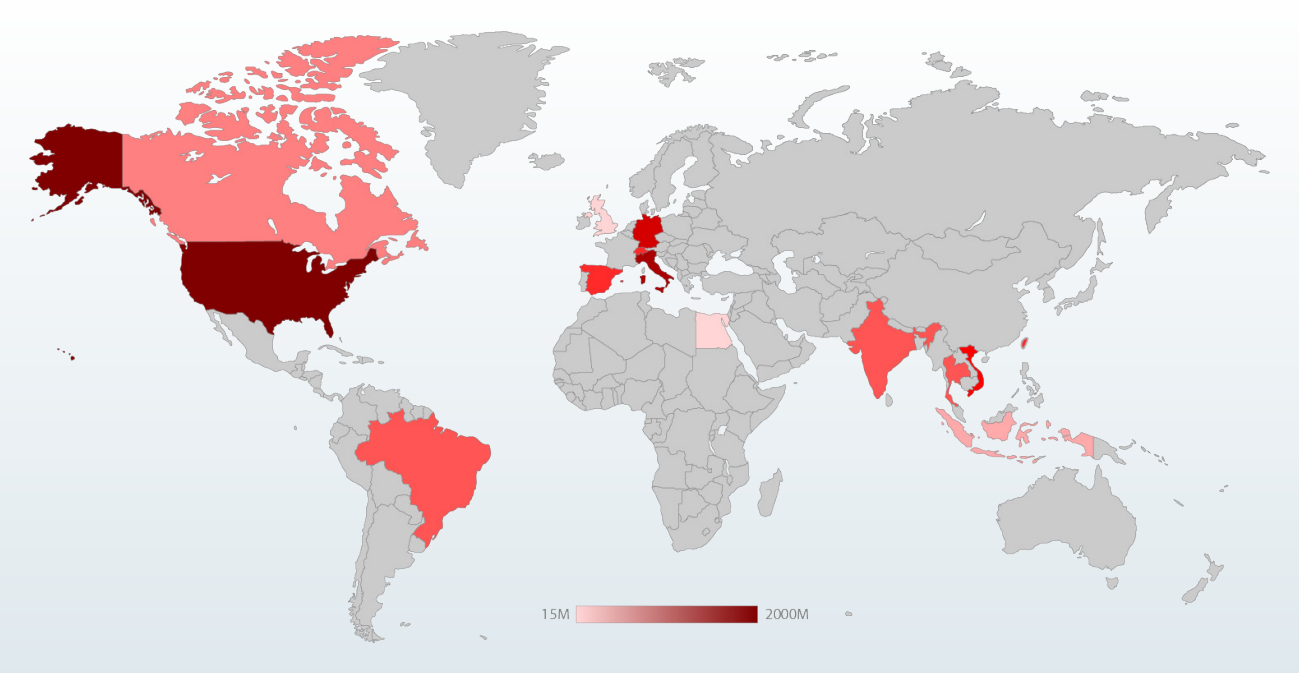


Figure 13: Origin of Bad Bots – World Map

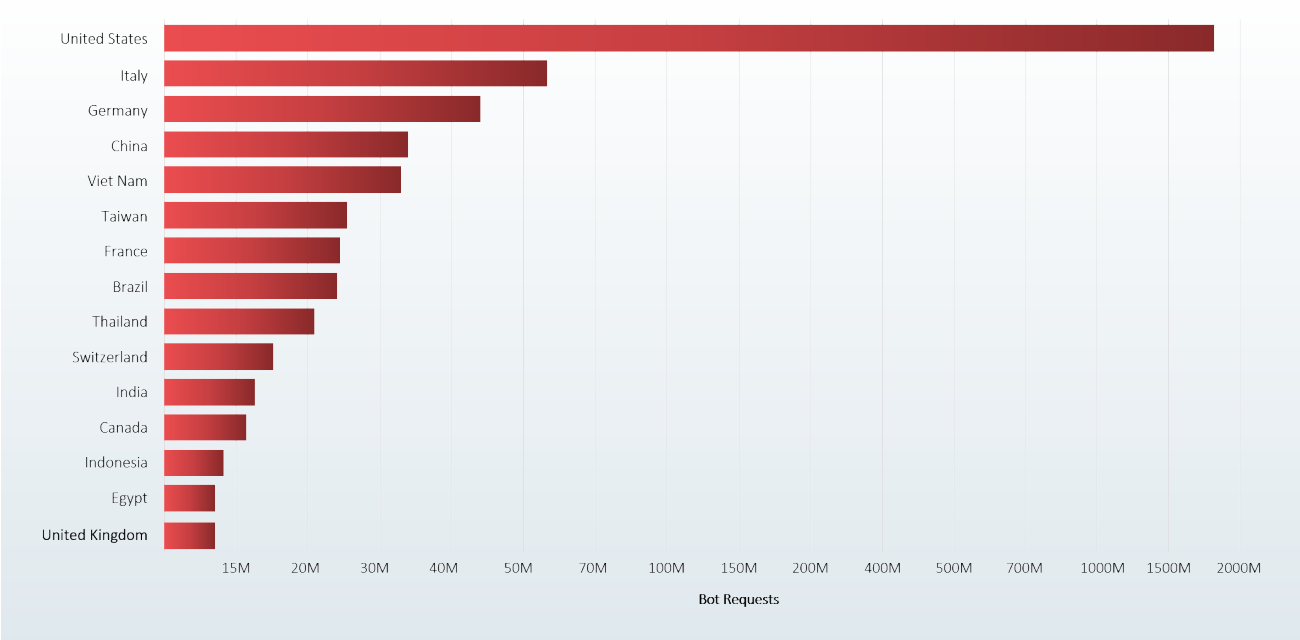
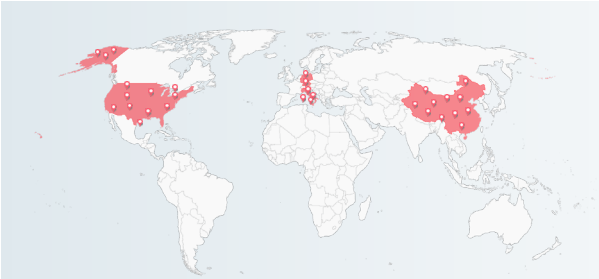


Figure 14: Origin of Bad Bots – by country



Most of the bad bots originated from the US, followed by Italy, Germany, and China

Four Major Threats to E-commerce Firms from Bad Bots

- Login pages are the most targeted pages of e-commerce firms to take over user accounts or create fake accounts.
- Cart abandonment by bots is another threat that e-commerce businesses are facing from bots, followed by scraping of unique content and carding.

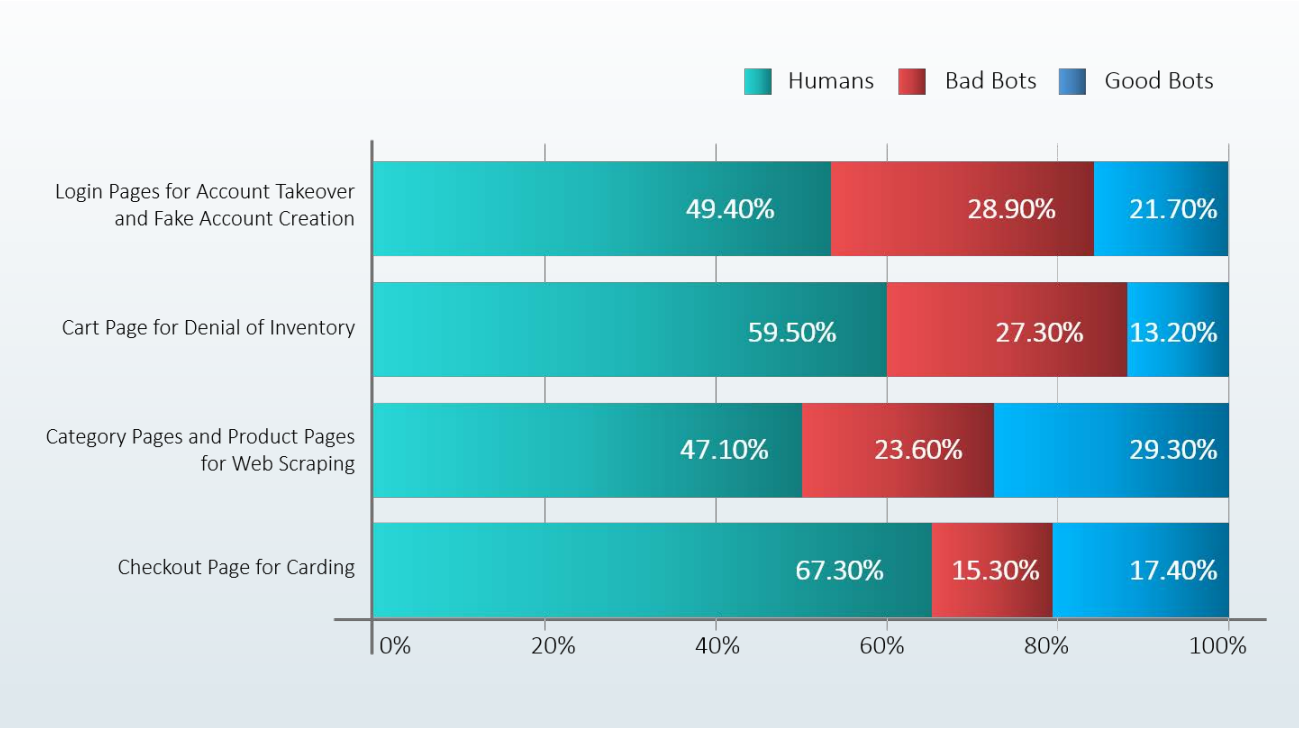


Figure 15: Four Major Threats to E-commerce Firms from Bots

Recommendations

All large e-commerce platforms have sophisticated bot activity on their website, mobile apps, and APIs that can expose them to account takeover, content scraping and loss of Gross Merchandise Value (GMV). E-tailers must be diligent in their approach to find and mitigate malicious sources of bot activity.

Build Capabilities to Identify Automated Activity in Seemingly Legitimate User Behaviors

Sophisticated bots simulate mouse movements, perform random clicks, and navigate pages in a human-like manner. Preventing such attacks requires deep behavioral models, device/browser fingerprinting, and closed-loop feedback systems to ensure that you don't block genuine users. Purpose-built bot mitigation solutions detect such sophisticated automated activities and help to take preemptive actions. In comparison, traditional security solutions – such as firewalls and WAFs - are limited to tracking spoofed cookies, user agents, and IP reputation.

Also, building or deploying a dedicated bot management solution will allow you to restrict AuthBots on login pages which in turn can help in eliminating other types of automated attacks that are performed after logins such as web scraping, checkout abuse, and denial of inventory.

[*You may also like: Development of In-house Bot Management Solutions and their Pitfalls*]

Deploy Challenge-Response Authentication

Challenge-response authentication is one basic security protocol that can help you filter bad bots. There are different types of authentication using challenge-response authentication, CAPTCHAs being the most widely used one. Challenge-response authentication can help in filtering outdated user agents/browsers and basic automated scripts but won't assist in blocking sophisticated bots that mimic human behavior and can solve CAPTHCAs. Also, challenge-response authentication requires a risk scoring mechanism, as showing multiple CAPTCHAs to users disrupts the customer experience.

[*You may also like: Sorry Google, No CAPTCHA reCAPTCHA Doesn't Stop Bots*]

Block Bad Bot Harboring Public Clouds/Data Centers

Data centers/public cloud service safe harbor bad bots. Organizations can block suspected data centers/public cloud services and ISPs. However, blocking all the traffic coming from data centers or ISPs without considering the user behavior can cause false positives. For example, a significant number of users on digital publishing sites come from commercial organizations that use secure web gateways (SWGs) located in data centers to filter user-initiated traffic[1]. Blocking data center traffic without considering domain-specific user behavior can cause false positives for digital publishing sites.

[*You may also like: Why Blocking Data Center Traffic to Prevent Bots Ends Up Blocking Real Users Too*]

Monitor Failed Login Attempts and Sudden Spikes in Traffic for AuthBot Attacks

Cyber attackers deploy bad bots such as AuthBots to perform credential stuffing and credential cracking attacks on login pages. Since such approaches involve trying different credentials or different combinations of user IDs and passwords, it increases the number of failed login attempts. The presence of bad bots on your website (to perform scraping, account takeover, or any other type of automated activity) suddenly increases the traffic. Monitoring failed login attempts and a sudden spike in traffic can help organizations take preemptive measures before bad bots cause any damage.

[*You may also like: How Massive Data Breaches Are Fueling Account Takeover Attacks*]

Spot Highly Active New or Existing User Accounts that Don't Buy

E-commerce portals must track old or newly created accounts that are highly active on the platform but haven't made any purchase in a long time. Such accounts may be handled by bots that mimic genuine user behavior to scrape product details and pricing information.

[*You may also like: Stepwise Analysis of a Large-Scale Scraping Attack on an E-commerce Website*]

Don't Overlook Unusual Traffic on Selected Product Pages

E-tailers should monitor unusual spikes in page views of certain products. These spikes can be periodic in nature. A sudden surge in engagement on selected product pages can be a symptom of non-human activity on your website.

[*You may also like: How Scraping Attacks Can Compromise Web Security and Impact Business Continuity*]

Watch Out for Competitive Price Tracking and Monitoring

Many e-commerce firms deploy bots or hire professionals to scrape product details and pricing information from their rival portals. You must regularly track competitors for signs of price and product catalog matching.

[*You may also like: E-commerce Portals Are Attacked with Distributed Multi-stage Scraping Attacks: ShieldSquare Research*]

Related Content

1. The Ultimate Guide to Bot Management
2. How to Evaluate Bot Management Solutions
3. Development of In-house Bot Management Solutions and their Pitfalls
4. The Big, Bad Bot Problem Q1 2019

About Radware

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019.

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

radware | SHIELDSQUARE

www.radware.com | www.shieldsquare.com

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.

© 2020 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.