kasada

2022 Holiday Bot Threat Report

Analysis of Bot Activity on Black Friday & Cyber Monday

Introduction

The **2022 Holiday Season Bot Threat Report** compiles threat intelligence data during the month of November to demonstrate how automated threats impacted holiday sales. Kasada processed over 6.8 billion eCommerce requests and over 400 million bad bot requests. Kasada protects some of the largest global retail brands and safeguards $50+ billion in eCommerce, $10+ billion in gift cards, and 2+ billion accounts globally.

eCommerce Holiday Traffic Processed

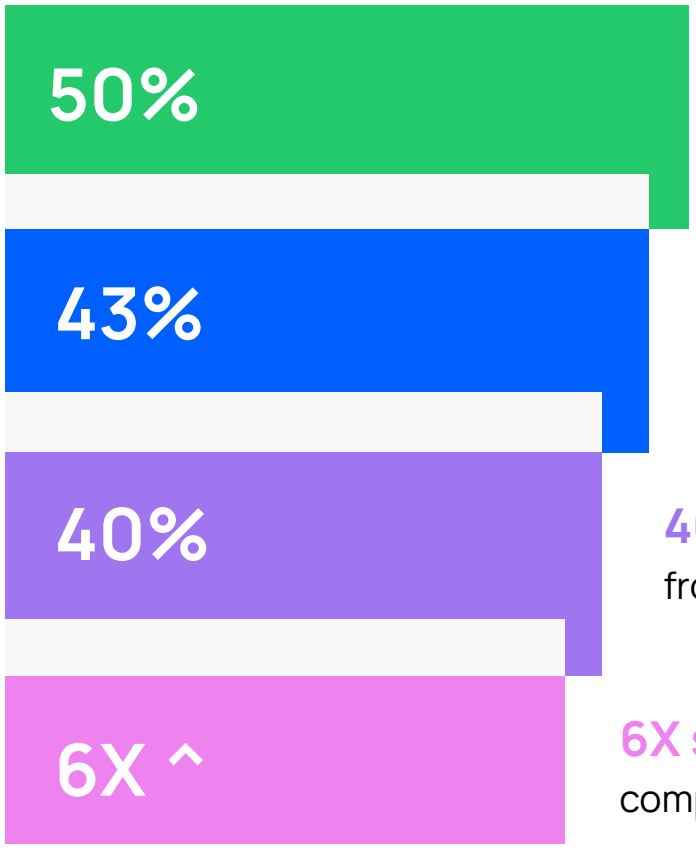
Total Requests	Bad Bot Requests	% of Traffic = Bad Bots
6,877,984,899	400,720,729	5.8%

Key Findings

Bots Ramped Up Attacks During Holiday Cyber Sales

Through processing over 6.8 billion requests, Kasada observed a 23% increase in bad bot traffic in the week before Thanksgiving and a 50% increase during Black Friday week.

Kasada's Threat Intelligence team identified four major cyber threats to retailers this holiday shopping season. Our data reveals a surge in scraping attacks, Freebie Bots, fake account creation, and gift card fraud. Bot operators frequently used open-source dev tools, spoofed browser platforms, and headless browsers to perform their attacks at scale.



50% increase in bad bot traffic the week of Black Friday

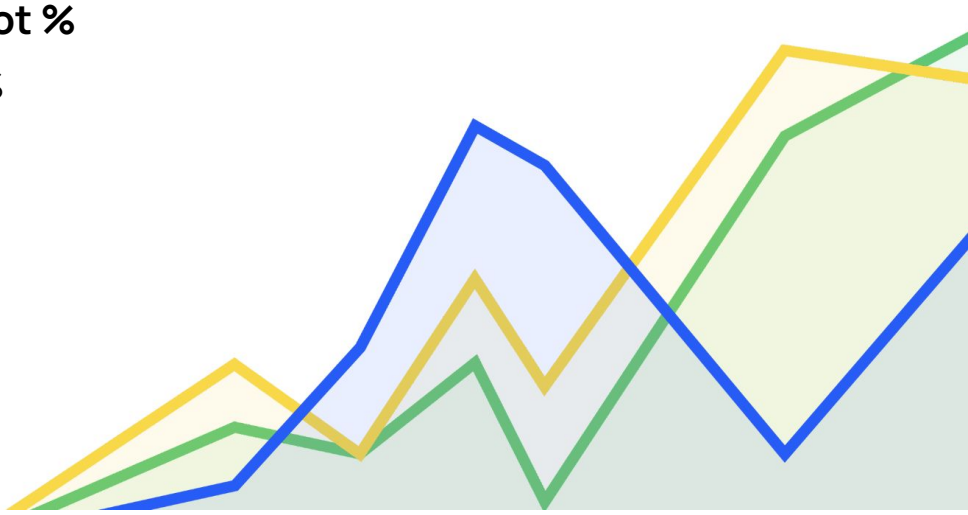
43% increase in scraping attacks, Freebie bots made $1M worth of products

40% increase in fake account generation from Black Friday to Cyber Monday

6X spike in gift card lookups every weekend compared to just hours prior to the attack

Bad Bot Traffic by Country of Origin

	Country	Total Bot %
1.	United States	49%
2.	United Kingdom	10%
3.	Canada	7%
4.	Australia	6%
5.	Korea	5%
6.	Denmark	4%
7.	Japan	3%
8.	China	3%
9.	France	2%
10.	Netherlands	1%



Scraping Attacks

43% Increase in scraping attacks leading up to Black Friday and over **3 million scraping requests** per day during peak times

43%
Increase in scraping attacks

11.5M+
Scraping requests a day

3M+
Scraping requests a day

Rather than target specific product pages, bots indexed entire websites, leading us to believe their goal was to monitor stock and price changes for arbitrage. Scrapers are a common reason why websites suffer slow speeds and degraded site performance.

Around the holidays, this is particularly troublesome for retailers since conversion rates are on the line and websites are already inundated with higher traffic volumes.

Freebie Bots

Bots Ramped Up Attacks During Holiday Cyber Sales

Freebie Bots leverage automation to scan retail websites for mispriced or discounted goods and purchase them at scale before the error is fixed.

Freebie Bots were drawn to Black Friday and Cyber Monday deals to score items at a fraction of the price and then resell them for a profit. Products with the highest discounts (70%-100% off) offered botters the best profit margin and were subsequently the most desirable. Items purchased by Freebie Bots typically weren't high-value items or in high demand, but rather ordinary consumer products such as LED strips and dog collars.

Kasada estimates that Freebie Bots successfully purchased over 40,000 products during Cyber 5 week (11/17 to 11/29), totaling over $1.1M in retail value for a small price of $134. Earlier in the month, a group of Freebie bots targeting a single retailer was solely responsible for obtaining over $500,000 worth of goods (over 20,000 products) that cost the bot operators only $85.

Leading up to Black Friday, bot checkouts steadily increased daily, with spikes occurring at 12:00 a.m. PST on Thanksgiving and Black Friday. Data suggests retailers had products scheduled to go live at midnight and once product became available, Freebie Bots quickly identified pricing and checked-out.

Freebie Bot Checkout Success

November 17th - November 29th , 2022

$1.1M+	40,000+	$134
Total Retail Value	# of Products	Total Paid

Fake Account Generation

3X increase

In fake account creation by bot uporation leading up to Black Friday

Kasada's Threat Intelligence team observed large amounts of new accounts generated a week before Black Friday and on Cyber Monday. New accounts are typically created by bad actors using free email providers like iCloud and Gmail to create fake accounts and circumvent inventory checks during checkout.

A 3x increase in fake account creation before Black Friday suggests that adversaries were preparing for holiday sales and hype drops by aging fake accounts. Bot operators "age" accounts by creating fake user accounts days before a sale starts to avoid detection and increase the likelihood of securing products. Aged accounts are either used for personal gain or sold to other parties.

From Black Friday to Cyber Monday, the number of fake accounts generated rose by 40%. We suspect fake accounts were used to commit new account fraud and take advantage of sign-up promotions. The better the incentive, the more likely bots are to create massive volumes of new accounts to claim the free product or coupon.

▲ 40%

in fake accounts created by bot operators between Black Friday & Cyber Monday

Gift Card Fraud

40% Spike in Gift Card Fraud Every Saturday

Throughout the holidays, fraudsters regularly check balances by performing automated gift card lookups.Kasada has observed a 6x increase in gift card lookups over the span of a few hours during weekend holiday shopping in November.

Last year, gift card lookups quadrupled, which was an early warning sign and a key indicator that fraudsters were using bots to quickly identify and steal the remaining balances on gift cards at scale.

A Better Solution

Kasada enables companies to increase their return on investment (ROI) and reduce their total cost of ownership (TCO) with the most effective and easiest to use bot mitigation platform – with no rules, no ongoing management, and no headaches. Unlike legacy rule-based solutions, Kasada is easy-to-use and offers long-lasting protection from across web, mobile, and API channels.

Our invisible defenses eliminate the need for CAPTCHAs, ensuring a frictionless user experience in their digital journey. Our proactive, dynamic platform adapts as fast as attackers do, making automated attacks unviable.

Learn how you can save time and money while protecting your revenue, customers, and brand at kasada.io.

About Kasada

Kasada has developed a radical approach to defeating automated cyberthreats based on its unmatched understanding of the human minds behind them. The Kasada platform is intentionally engineered to overcome the shortcomings of traditional bot management tools. Kasada is based in New York and Sydney, with hubs in Melbourne, Boston, and San Francisco. For more information, please visit www.kasada.io and follow on Twitter, LinkedIn, and Facebook.

Copyright 2023, Kasada, Inc. All rights reserved.