kasada

2023 Holiday Bad Bot Report

Overview

The 2023 Holiday Bad Bot Report compiles online traffic and data from September to November to demonstrate how automated threats, bot attacks, and online fraud impacted eCommerce and holiday sales.

Kasada processes billions of human and bot traffic requests while protecting some of the largest retail brands in the world. Kasada safeguards $150+ billion in eCommerce, $10+ billion in gift cards, and 2+ billion accounts globally.

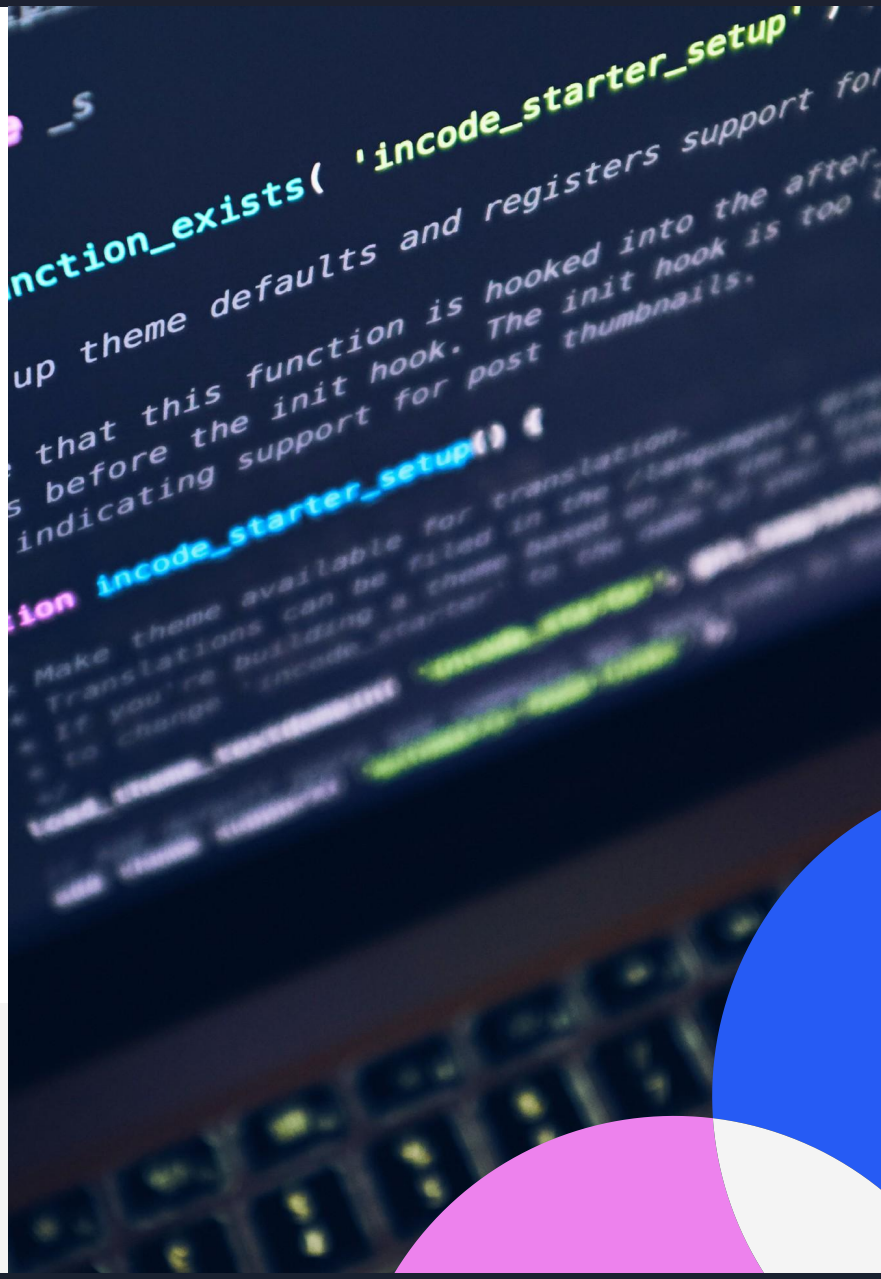
Overall Holiday Traffic Comparison 2023 vs. 2022

Total Traffic:
▲ +44% from 2022

Total Bad Bot Traffic:
▲ +283% from 2022

% of Bad Bots to Humans:
▲ +198% from 2022

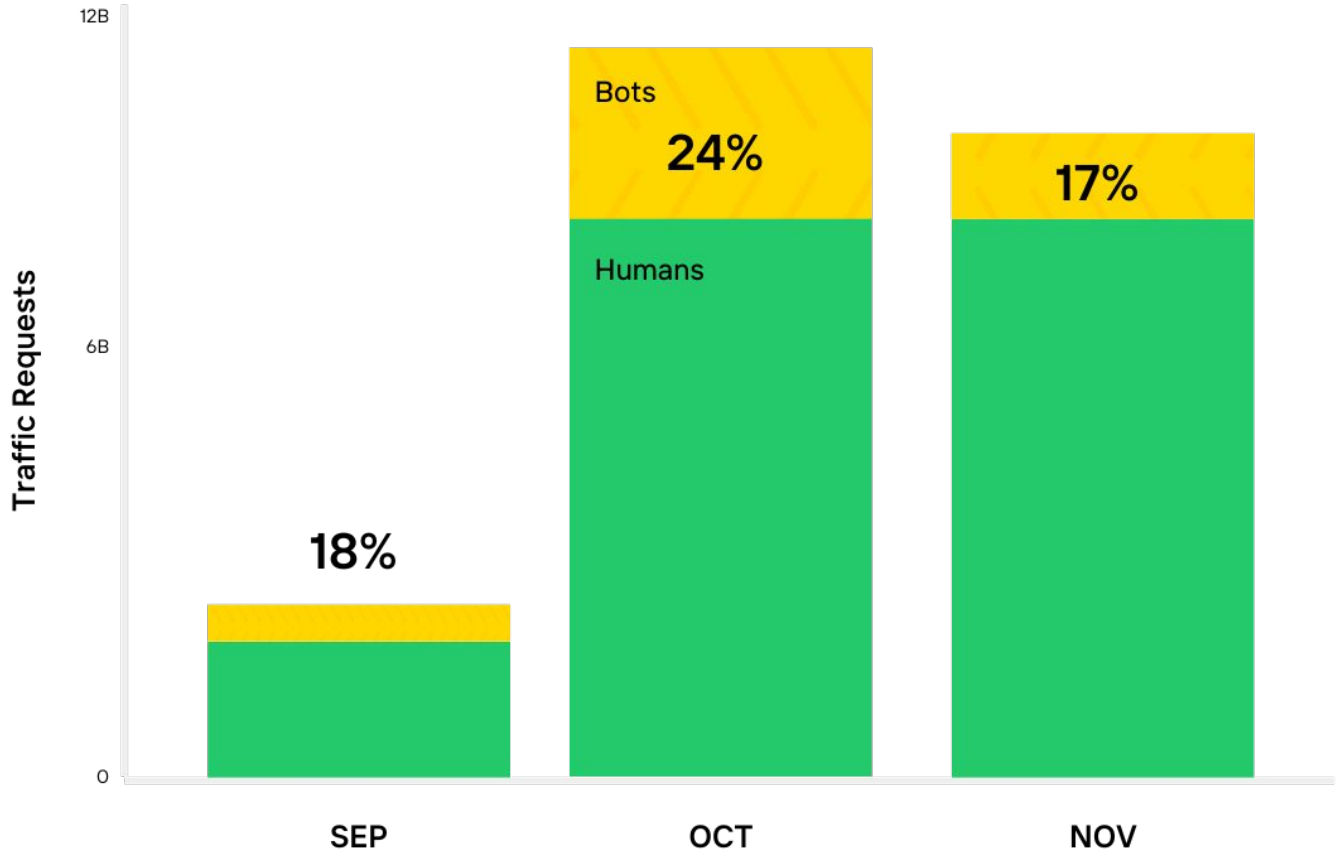
> The ratio of bot traffic to human traffic grew **198%** in the 2023 holiday season so far compared to 2022.



Key Findings

Bots Ramped Up Attacks Before Holiday Cyber Sales

Despite booming holiday sales around Thanksgiving Day in the United States, Kasada processed more human and bot traffic in October than November - suggesting early bird holiday sales were popular for retailers, legitimate consumers, and adversaries alike. In fact, overall bot traffic requests grew by 444% (5.4x) from September to October, and then declined by 50% in November.



Key Findings (Continued) →

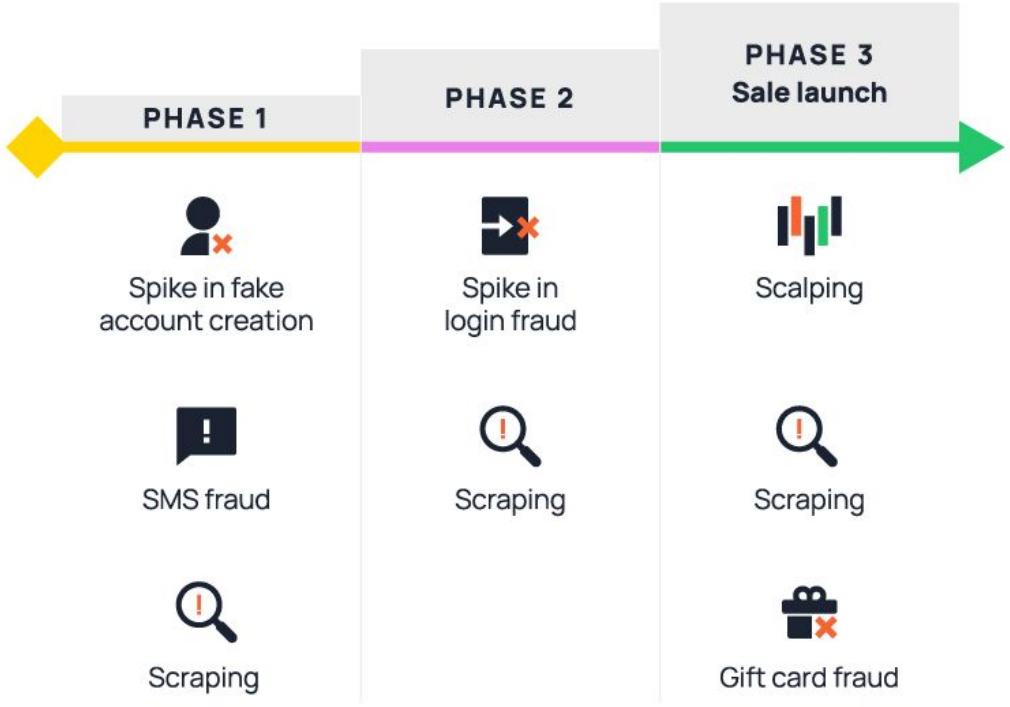
Key Findings (Continued)

Adversaries Strategically Deployed Specific Attacks Before and During Holiday Sales

When analyzing specific types of attack vectors relative to sales events, adversaries used bots to perform fake account creation, credential stuffing, and scraping attacks prior to online holiday sales. During peak sales periods in November, bots were most used for scalping, login abuse, and gift card fraud.

Before peak holiday sales: Adversaries attempted to create and age fake accounts before sales started, which is a common occurrence for hype releases that helps ensure bot operators have more chances to score in-demand products. Adversaries also attempted to test stolen login credentials in the days leading up to sales events. Data scraping was another popular attack both before, during, and after sales to monitor inventory and price changes.

During peak holiday sales: Scalping, automated account login attempts, and gift card fraud seemed to occur most during peak sales. In a given day, scalping made up 63% of all bad bot requests, and automated login requests increased by 250% from November 25th to November 26th. During the Cyber Five weekend, a spike in gift card fraud occurred on Black Friday and Cyber Monday.



“Cyber Five” Overall Bot Traffic

THANKSGIVING, NOVEMBER 23 TO TRAVEL TUESDAY, NOVEMBER 28

Bot to human traffic comparison: 12%

Peak Botting Activity:

Wednesday, November 22, 2023

Surprisingly, the peak of bot activity didn’t happen on Cyber Monday or even Black Friday. What we observed is that Wednesday, November 22 which is the day before American Thanksgiving, had the most bad bot requests during Cyber Week. We attribute this to pre-holiday sales that bots are privy to before real shoppers, as **63%** of those bot requests were scalper bots.

During the “Cyber Five” weekend, the most popular botting days were Black Friday, Cyber Monday, and Travel Tuesday.

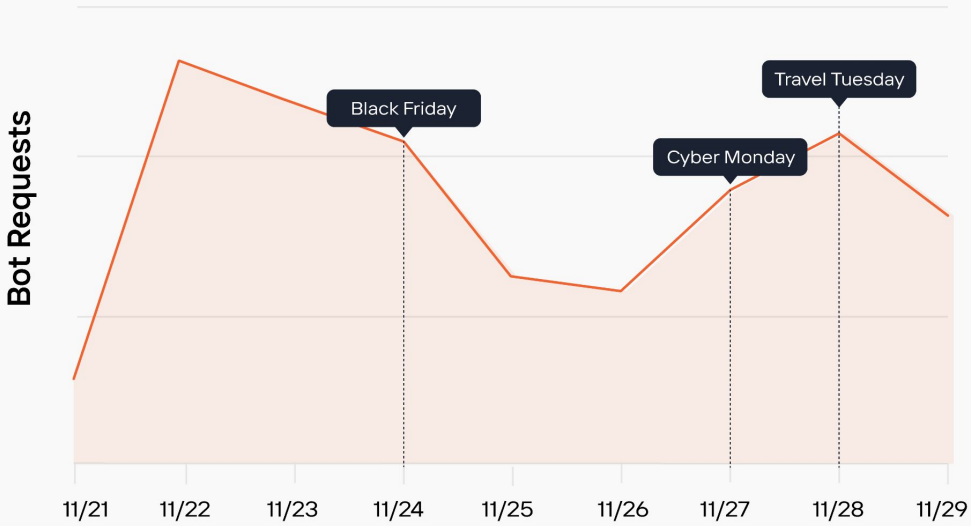
For humans, peak shopping activity really started on Black Friday. Shoppers seemed to do most of their online shopping on Black Friday, then on Cyber Monday. In fact, Black Friday received 12% more legitimate human traffic than Cyber Monday.

12%

Human traffic was 12% higher on Black Friday than Cyber Monday.

Cyber Week Bot Requests

Day-by-day traffic comparison (2023)



Most Bot Requests:

1. Black Friday, November 24
2. Cyber Monday, Nov. 27
3. Travel Tuesday, Nov. 28

Most Human Requests:

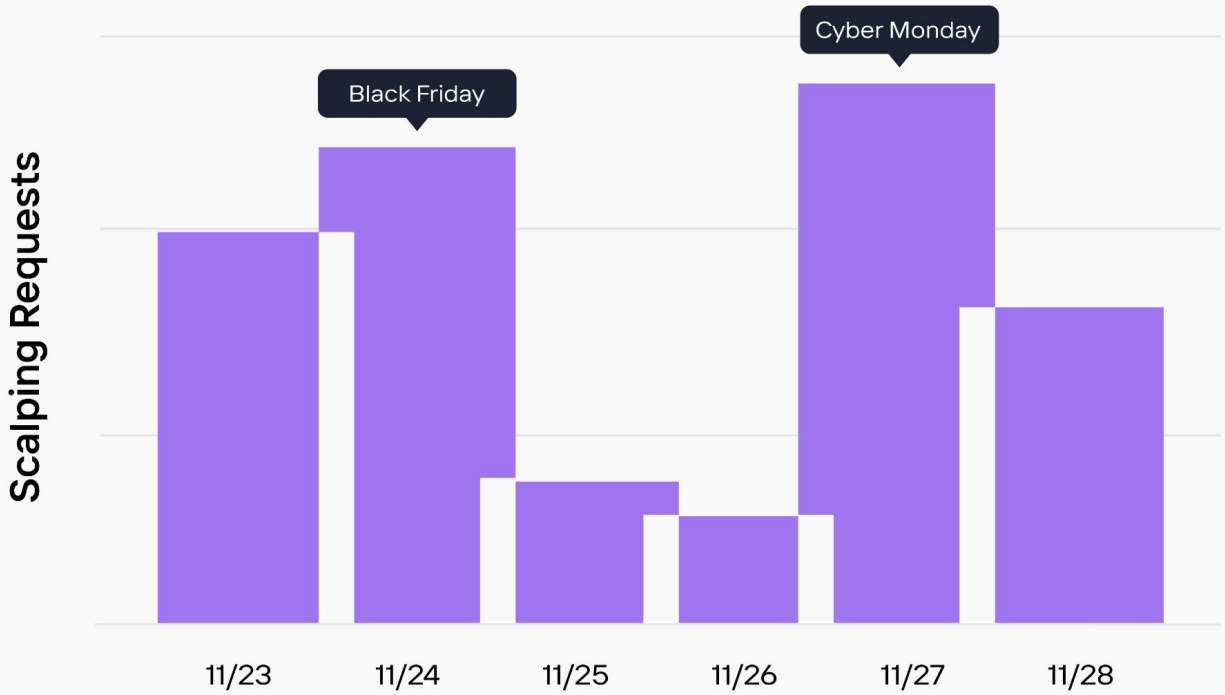
1. Black Friday, Nov. 24
2. Sunday, Nov. 26
3. Cyber Monday, Nov. 27

Cyber Five Deep Dive →

“Cyber Five” Deep Dive: Scalper Bots

3X Surge in Grinch Bots on Cyber Monday

After their early start before “Cyber Five” weekend, Grinch Bots continued to plague holiday sales through the weekend - favoring Cyber Monday and Black Friday sales. Scalping requests spiked by 3x on Cyber Monday as they attempted to purchase sale items before most humans were even awake.



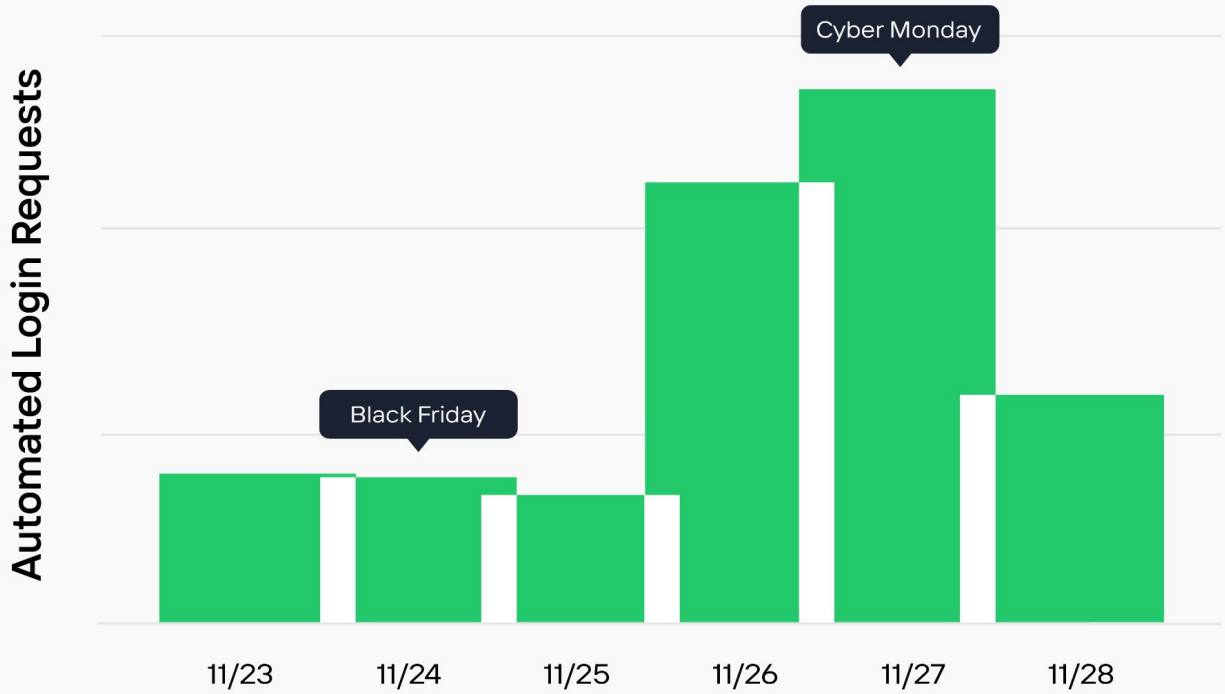
51% of bot requests on Black Friday were scalpers, also known as Grinch Bots.

Grinch bots often used advanced open source tools like Puppeteer Stealth and Playwright to conduct scalping attacks.

“Cyber Five” Deep Dive: Account Login Fraud and Abuse

3X Surge in Automated Login Attempts on Cyber Monday

Grinch bots weren’t the only popular attack during the “Cyber Five” weekend. After a few days of sales, adversaries increased efforts to hack into accounts. Kasada observed a 3x surge in automated login requests on Cyber Monday compared to earlier in the week. Had adversaries been successful in stealing customer accounts, orders might have been mysteriously rerouted, or fraudulent orders could have been placed. Having proper cyber defenses in place at the login to safeguard against automated login attempts helps protect more consumers against fraud and added stress to their holiday shopping.



251% increase in login fraud attempts from Saturday, November 25th to Sunday, November 26th.

“Cyber Five” Deep Dive: Adversarial Sophistication

Over Half of Attacks Used Highly Advanced Tools and Techniques

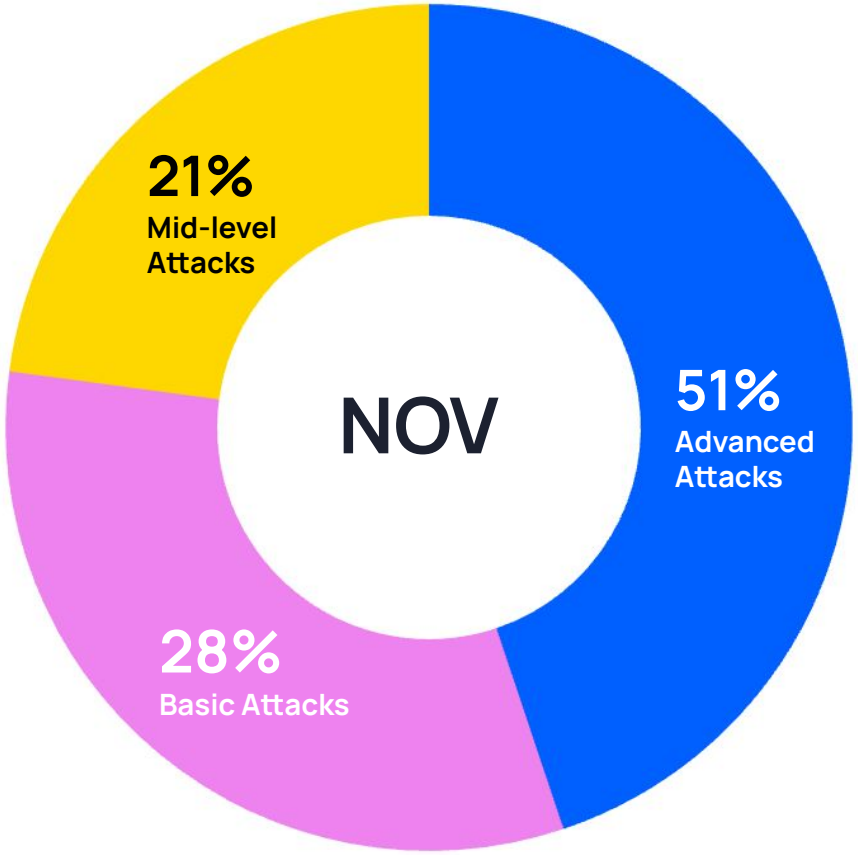
51% of the observed holiday bots were highly sophisticated, utilizing advanced tools such as Puppeteer Stealth. In contrast, 21% employed mid-level techniques, and 28% used basic tools.

The differentiation in attack techniques is noteworthy. For instance, scalpers, who are likely involved in manipulating online prices and inventory, often employ advanced tools to bypass detection mechanisms. On the other hand, attacks related to SMS and gift card fraud tend to use less sophisticated tooling.

To safeguard their data and customers during peak sales periods, eCommerce and retail organizations must be proactive in defending against advanced tooling. It’s crucial to anticipate that adversaries will continue to evolve their tactics, testing defenses, reverse engineering security measures, and experimenting with different methods.

Level of bot sophistication:

- 51% of bots used highly sophisticated techniques and tools, such as Google Puppeteer and Microsoft Playwright.
- 21% used mid-level sophistication techniques and tools, such as fake browser attacks.
- 28% used simple techniques and basic tools, such as fake Google bots or cURL commands.



November Bot Traffic

Bot to human traffic comparison: 17%

3.7x Increase in Gift Card Fraud

In November, Kasada witnessed a steady rise in gift card fraud attempts. This marked a massive 3.7x increase compared to October. With eCommerce merchants and retailers launching holiday sales and promotions, this makes it a prime time for cybercriminals to exploit any weaknesses in gift card generation or validation processes. Bots can be deployed to rapidly test and exploit various combinations of gift card codes in an attempt to find valid ones that can be used or sold on secondary markets.

Automated login attempts were also more common in November, increasing by 7% from October to November. On one day in particular, November 8, automated login attempts increased by a staggering 15x, suggesting a credential stuffing or account takeover attack was underway.

Stolen accounts around the holidays are lucrative for adversaries, as more cybercriminals are looking to purchase them to secure the hottest products of the season, take advantage of early access member-only deals, steal loyalty points, and commit fraud. In fact, in early November, Kasada observed over 100,000 accounts were purchased on cybercriminal marketplaces from top retailers in a matter of days.

Retailers should be vigilant during the holiday season, implementing robust security measures to detect and prevent automated attacks on gift card systems, login endpoints, and checkout processes, protecting both their business and their customers from fraudulent activities.

One day in particular, November 8, automated login attempts increased by a staggering **15x**.

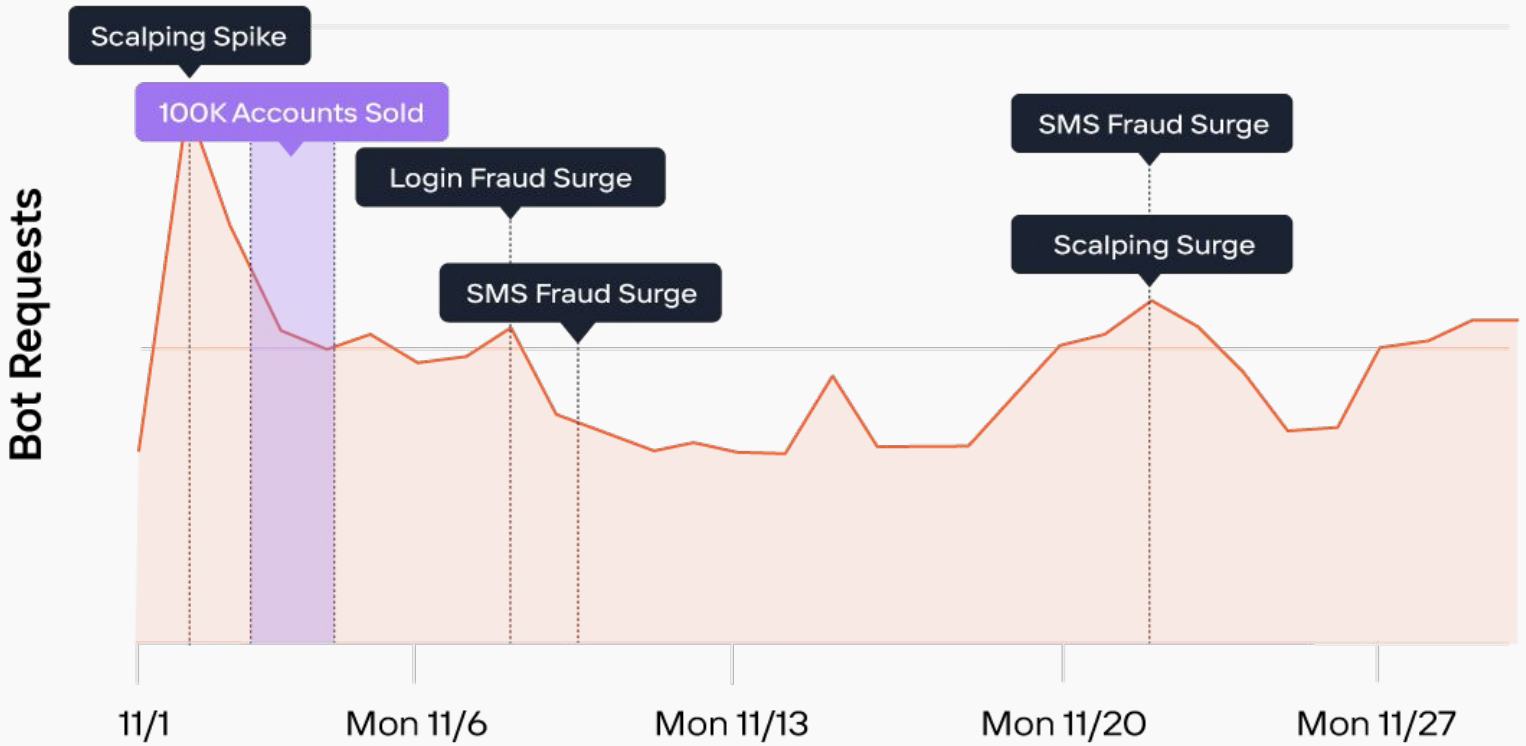
Kasada observed over **100,000 accounts** were purchased on cybercriminal marketplaces from top retailers in a matter of days.

November Bot Traffic

100,000+ retail accounts sold in a matter of days

7% increase in automated login attempts

3.7x increase in gift card fraud attempts



October Bot Activity

Bot to human traffic comparison: 24%

5.4x Increase in Bad Bot Activity in October 2023

October saw the highest levels of bot activity, compared to September and November 2023. In October, Kasada processed billions of human and bot requests, all of which seemed to correlate with early-bird holiday sales.

Bot activity grew an alarming 5.4x from September to October, with bots making up 24% of all traffic requests. This is double the amount of bot-to-human traffic than what was observed during the Cyber Five weekend.

Those looking to score a profit during pre-holiday sales followed a pattern of behavior just like during the Cyber Five holiday weekend. Prep work was done beforehand to age new accounts, test credentials to steal account information, as well as scrape prices, product catalogs, and inventory. In one week of October, fake account creation attempts increased by 3.4x.

Scalper bots seemed to hit the most during early to mid-October when we suspect holiday sales first started. The level of sophisticated attacks during this time period rose, switching from tactics like fake browser attacks to Puppeteer Stealth. Kasada saw a massive 541% increase in scalper bot activity from September to October.

When planning both pre-holiday and holiday sales, businesses should expect bots to take advantage of the promotions. Bot attacks like scalping, scraping, fake account creation, credential stuffing, and gift card fraud are all popular adversarial attack vectors, and they require protection across each endpoint.

Bot activity grew an alarming **5.4x** from September to October.

In one week of October, fake account creation attempts increased by **3.4x**.

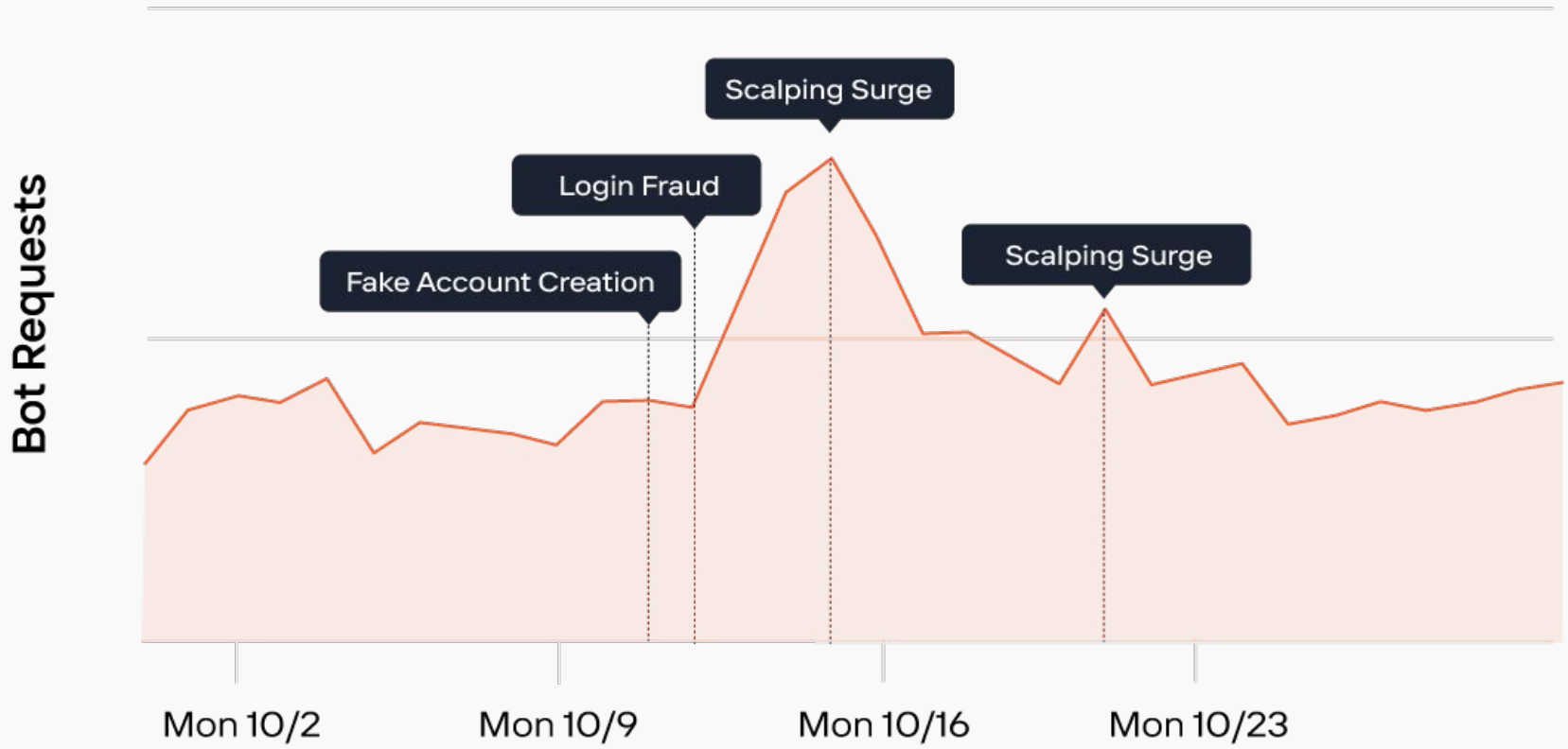
Kasada saw a massive **541%** increase in scalper bot activity from September to October.

October Traffic Breakdown

5.4x increase in bot activity from September to October

3.4x increase in fake account creation attempts in one week

4x increase in overall traffic from September to October



Takeaways and Recommendations

Key Insights to Take Away

- **Early Fraud Activity:** Threat actors initiate fraudulent schemes and tactics well before peak sales seasons, including Black Friday and Cyber Monday holiday sales.
- **Year-Round Scraping:** Price, content, and API scraping occurs all year long, so you need continuous vigilance against these attacks, no matter when your sales start.
- **Credential Stuffing for Account Takeover:** Bad actors employ bots to commit credential stuffing techniques early on in the peak sales season, targeting accounts to take over for maximum impact and profit.
- **Gift Card Fraud Timing:** Fraudsters check gift card balances after purchase but before gifting, emphasizing the need for early fraud detection.
- **New Account Fraud Lead Time:** Adversaries initiating fake account creation start early to age accounts so they can evade your security defenses.
- **Scalping During Sales Events:** Scalping peaks during major sales events, requiring heightened monitoring and bot protection.

Steps to Take to Protect Your Organization

1. **Behavioral Analysis for Traffic Spikes:** Monitor unusual traffic spikes, especially at critical endpoints.
2. **Endpoint Targeting and Distributions:** Identify and flag abnormal traffic, such as rapid account creations or clusters of accounts sharing the same phone number or other common properties.
3. **Traffic Pattern Analysis:** Scrutinize overall traffic patterns, noting irregularities like the absence of a day/night cycles in your organizations' operating time zones.
4. **Routine Testing of Security Measures:** Regularly challenge and test anti-fraud, anti-bot, and business logic security services to ensure ongoing effectiveness.
5. **Internal Collaboration and Working Groups:** Foster collaboration cross-functionally including across e-commerce, security, fraud, and payments teams to enhance overall security measures. Recognize the importance of working groups in combating adversaries who are highly collaborative.
6. **Continuous Monitoring and Testing:** Think like an adversary; challenge internal processes, tools, and services to identify and adapt to evolving threats.

About Kasada

Kasada has developed a radical approach to defeating automated cyber threats based on its unmatched understanding of the human minds behind them. The Kasada platform overcomes the shortcomings of traditional bot management to provide immediate and enduring protection for web, mobile, and API channels. Its invisible, dynamic defenses provide a seamless user experience and eliminate the need for ineffective, annoying CAPTCHAs. Our team handles the bots so clients have freedom to focus on growing their businesses, not defending it. Kasada is based in New York and Sydney, with hubs in Melbourne, Boston, San Francisco, and London. For more information, please visit www.kasada.io and follow on LinkedIn, X, and Facebook.

Contact us:
enquiries@kasada.io
Australia: 1300-768-601
USA: 877-473-5073
kasada.io