kasada

Quarterly Threat Intelligence Report

Q3 | 2025

Introduction

Kasada's Q3 2025 (Q3) Threat Intelligence Summary arms you with the contemporary observations and assessments you need to meet the evolving challenges set by automated threats. With millions of unique events collected by Kasada IQ each quarter, this Threat Intelligence Summary cuts through the noise and pulls out the key areas your organization needs to focus on to stay ahead of the curve. All insights are based on analysis and investigations via our in-house Kasada IQ intelligence capability, supported by deep access to open and closed sources and decades of technical and intelligence expertise combined.

Intelligence Requirements

01

Which automated threat required the **most attention** in Q3?

02

What were the **top automated threats** observed by Kasada IQ in Q3?

03

What **movements** in the automated threat landscape did Kasada IQ observe in Q3?

04

How did the top threats observed by Kasada IQ in Q3 impact **key industries**?

How to read this report

Executive Summary
The key points you need to know from the report and how Kasada can help.

Spotlight On: Resurging Resellers
A deep dive into the resurgence of online reselling communities.

Threat Landscape Update
The top threats tracked by Kasada IQ over the past quarter and notable events across the landscape.

How we can help
How Kasada can help you beat the threats discussed in this report.

Table of Contents

Executive Summary

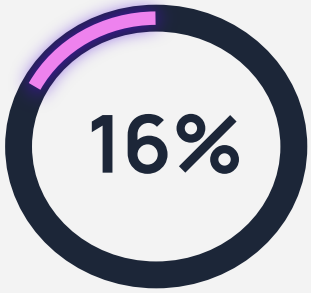
This report provides an overview of the automated threat landscape in Q3, with a particular focus on the resurgence of online reselling communities.

TOP THREAT

Account Takeover (ATO) remained the top threat.

Top Industries for Account Sales:

- Retail
- Quick Service Restaurants
- Webmail



Increase in observed account sales in Q3

Kasada IQ observed an anomaly in ATO activity that raised significant concerns. In Q3, three criminal marketplaces were selling accounts for both US-based **online gun dealers** and **WhitePages Premium** accounts. These kinds of accounts are not often targeted credential stuffing and ATO.

TOP INTENT CLASSIFICATIONS IN ATTEMPTED ATTACKS

API Automation | **Account Takeover** | **Checkout Fraud** | **Content Scraping** | **Fake Account Creation**

KEY OBSERVATIONS

In Q3, developments in the landscape demonstrated the need to **go beyond defensive monitoring and engage in proactive, bespoke defenses**. A big theme this quarter was structural resilience, with threat enablers (like proxy networks) obfuscating their activities and rapidly adapting their operations to maintain business continuity. This, combined with ongoing evolutions in the AI landscape, challenge traditional assumptions about adversary capability and attack sophistication. The developments emphasise the need to maintain traditional defenses, but **enhance with behavioral detection**.

Kasada's defense approach is **intelligence-led**. We gain deep insight into how attacks are planned, executed, and adapted. This intelligence allows us to build targeted, custom defenses that are informed by the specific threats facing your environment, not just generic patterns.

AI DEVELOPMENTS

The retail and eCommerce sectors are facing a new **AI-first** landscape with the rapid emergence of agentic AI browsers in Q3. Businesses are being driven to invest and ensure data is captured by AI. The normal things common for Search Engine Optimization (SEO) aren't captured by AI assistants.

AI relies on Q&A-rich, structured data that helps add context to answer. To stay competitive, eCommerce businesses are forced to **shift to Generative Engine Optimization (GEO)**. This further pushes the uptake of AI over classic search engines. With more people using AI browsers and assistants, **the attack surface for adversaries is expanding**.

ONLINE RESELLING COMMUNITIES

In both the Q1 and Q2 QTRs, Kasada IQ predicted and observed a resurgence of reselling communities and a refocusing on hype items. After a slow period in late 2024, economic pressures and trends within these reselling communities have reinvigorated the culture that drives these operations.

In Q3 alone, Kasada IQ observed nearly 75,000 bot checkouts across 8 specific hype items.

Economic uncertainty and tariffs are driving shifts in markets, supply chain and consumer behaviours. **Adversaries are capitalizing on these shifts**, purchasing up stock faster than any human and reselling at a significant markup. While reselling in some industries (like ticketing) is facing increased scrutiny, the majority of this activity is left unchecked.

The impacts of bots and online reselling communities goes beyond the immediate transaction, presenting a real threat to long-term health, brand loyalty and market stability.

Brand and reputation damage.

Fractured customer connections.

Artificial demand and adaptive adversaries.

The good news is that the online reselling cycle is predictable. The modus operandi for these adversaries is generally formulaic. They often operate through legitimate business structures, have a presence on the open web, communicate with their user base and offer their services or infrastructure for a fee. Adversaries in this environment are generally males aged 18 to 30 who leverage social media and online communities to showcase their successes and profits. These adversaries frequently positioning themselves as "influencers" in the "money-making" sphere. Although technology can help mitigate the business impact of these operations, long-term, sustained results depend on understanding human behavior.

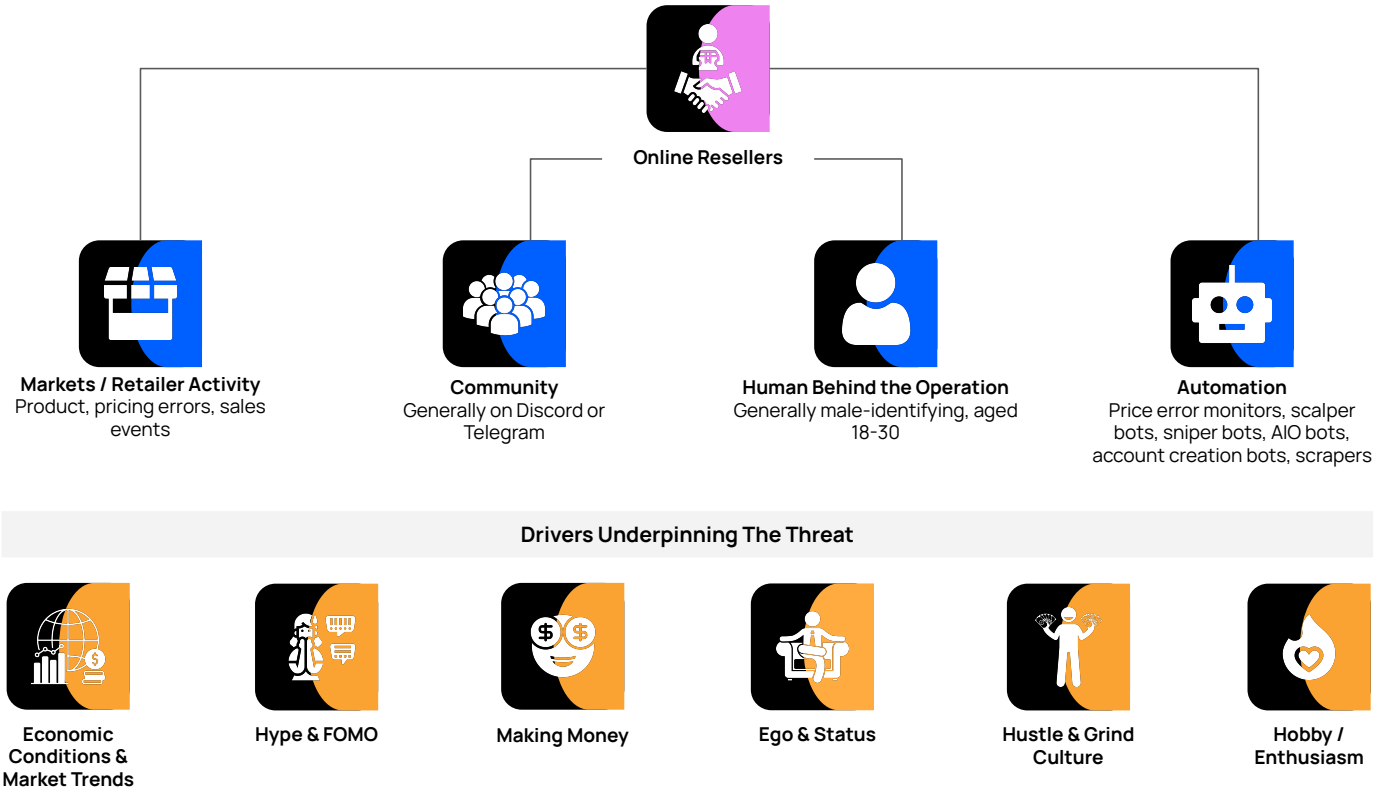
Kasada IQ focuses on the behavior behind the threat. Our intelligence considers the driving forces behind the threats: external influences, human behavior and community dynamics. By understanding the **psychology behind automated threats**, Kasada provides a sustainable and holistic approach to bot management.

Spotlight On: Resurging Resellers

In both the Q1 and Q2 QTRs, Kasada IQ predicted and observed a resurgence of reselling communities and a refocusing on hype items. In Q3 alone, Kasada IQ has observed **nearly 75,000** bot checkouts across **8** specific hype items. With significant long-term impacts for businesses and markets, online reselling communities will remain a threat to businesses as long as it remains profitable.

Kasada IQ considers **online resellers** to include communities serviced by automation software, commonly referred to as bots. These bots allow users to complete transactions much faster than any human. Bots are purchased and used by legitimate customers who use their own accounts and payment methods. The online reseller ecosystem operates on social platforms like Discord and Telegram. These communities provide resources and training to members and create a sense of social currency. These differ from non-automated resellers, including legitimate second-hand retailers, who rely on manual hunting and discovery in physical locations (like thrift stores) or on platforms like eBay.

This section deep dives into the online reselling ecosystem, identifying the key features, drivers and behaviors Kasada IQ is observing. It breaks down the common components, phases and drivers of the online reselling cycle and the different types of bots used to fuel it.



The Exclusivity Exchange

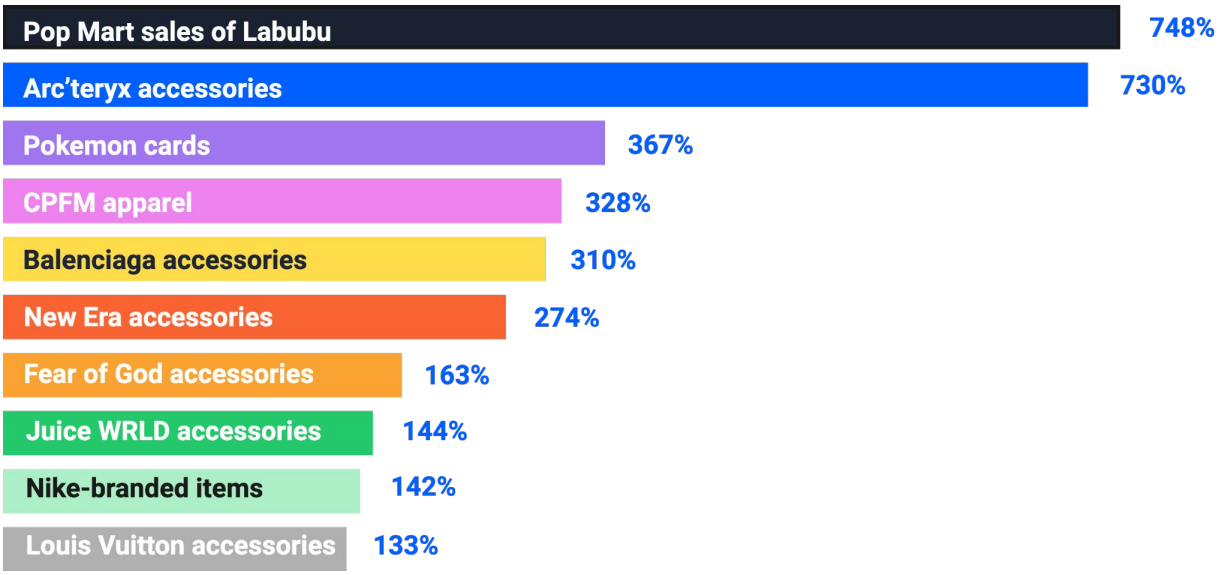
Kasada IQ observes that online reselling communities are frequented generally by young men influenced by the hustle and grind culture. After a slow period in late 2024, economic pressures and trends within these reselling communities have reinvigorated the culture that drives these operations. This resurgence aligns with broader consumer shifts towards second-hand goods and collectibles over traditional luxury items.

The luxury retail market is experiencing an interesting shift as noted in the True-Luxury Global Consumer Insights report from July 2025. The report indicated that the personal luxury market is facing a lack of growth for the first time in over a decade, a finding echoed by Bank of America in January 2025. The reports reveal that aspirational luxury customers (those spending under USD $6,000 a year) are diverting their spending away from luxury goods towards savings, investments, wellness and second-hand purchases.

The decline in first-hand luxury spending tracks with what Kasada IQ is observing online. In 2025, mentions of luxury are down 40% in online forums compared to 2024.

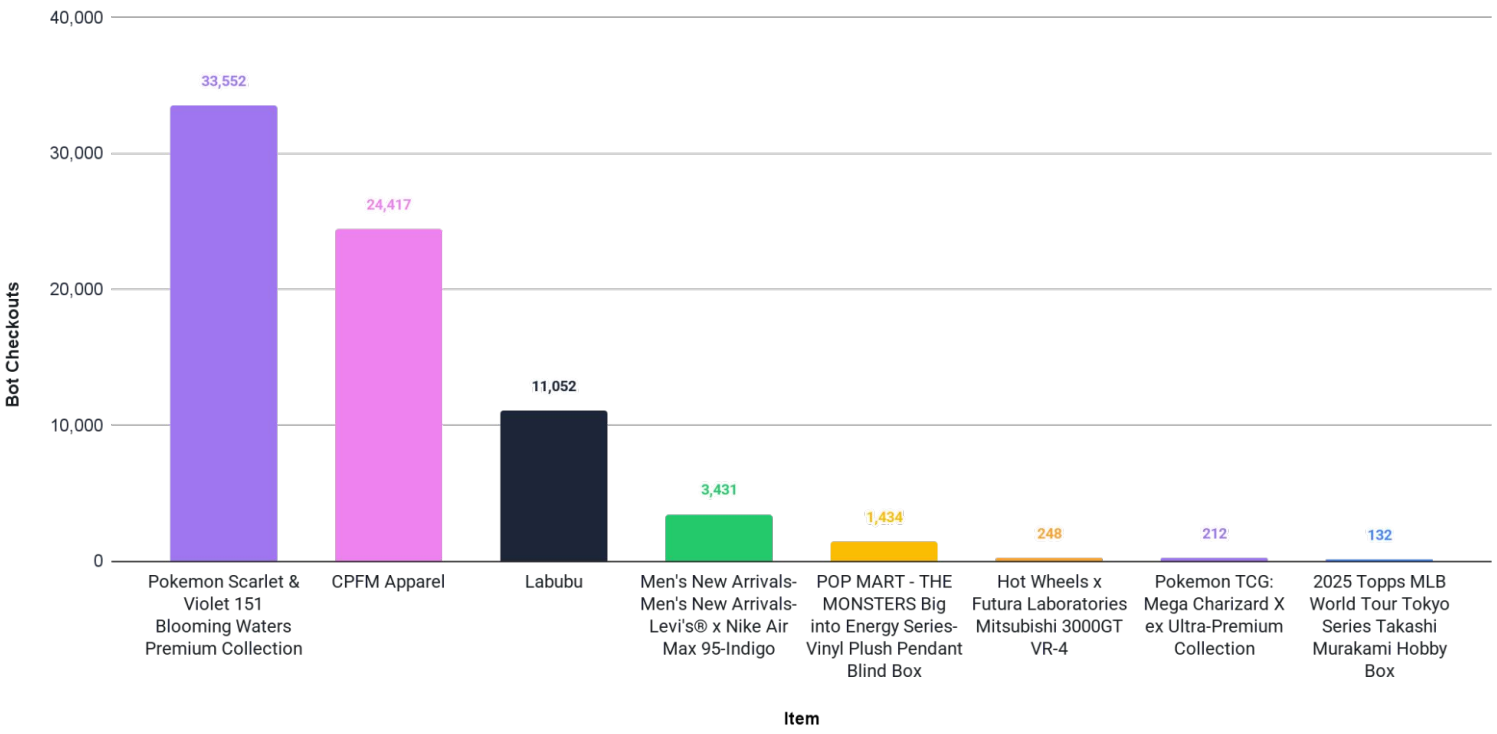
Consumers are demonstrating that you can get the same sense of exclusivity from collectible and second-hand items as you do for traditional luxury items. All of these categories provide an avenue for social signalling and self expression while offering a sense of belonging to consumers.

Like visits to thrift stores and second-hand franchises, trading on online marketplaces is significantly increasing. Some online marketplaces, like StockX, saw trade increases of up to **1 to 7 times** in the first half of 2025 when compared to the same period in 2024. The surge was particularly pronounced in collectible items. The three categories that saw the most growth were Pop Mart's Labubu figures (**748%**), Arc'teryx accessories (**730%**) and Pokemon cards (**367%**). Even established luxury brands like Balenciaga (**310%**) and Louis Vuitton (**133%**) experienced significant resale growth.



Source: StockX

Kasada IQ observed similar patterns to StockX within online reseller communities in Q3 2025. Several hype items received significant attention from buyers in online reselling communities. These hype items spread across a range of different categories, including trading cards, apparel and collectible toys. Similar to StockX, the top items for bot checkouts were Pokemon cards (**33,764** across both items listed below), CPFM Apparel (**24,417**) and Labubu (**11,052**).

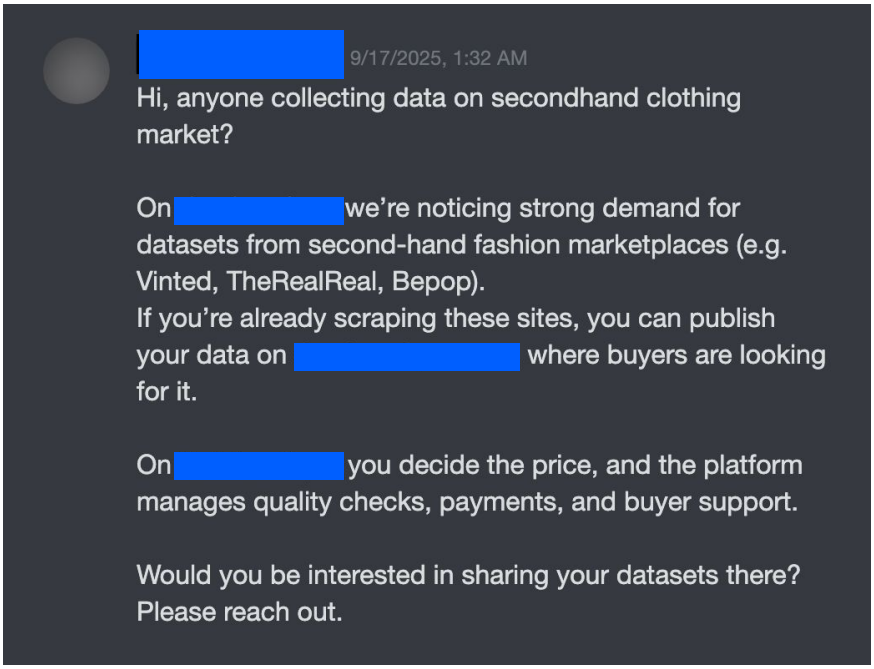


Hype items are limited-edition products from well-known brands that generate extraordinary demand through manufactured scarcity. By deliberately restricting supply, brands create exclusivity and drive significant secondary market premiums, transforming products into coveted status symbols.

Second-hand marketplaces aren't just a place for online reselling communities to resell goods. These marketplaces are **actively targeted by bots** that are specifically designed to monitor for opportunities to strike and continuously scrape valuable data (like pricing). Sneaker enthusiasts commonly publish open-source repositories for specific second-hand marketplaces, like StockX, on GitHub.

A primary focus for these bots is **sniping:** placing a last-second bid on an auction item. **Sniper bots** have features to give its users an advantage, like rapid price checking, price error monitoring, multiple wallets and floor price tracking.

While bots targeting second-hand marketplaces are available in open-source, there is also a secondary market for data harvesters and brokers. As show in the image below from an online community for web scraping, these kinds of brokers are demand-driven, closely monitoring patterns within second-hand and online reselling markets to drive their business strategy. They also rely on community contributions to drive their business. With scraping the core tool for these brokers, they are monetizing data driven by other businesses and resellers.



INVESTING THROUGH UNCERTAINTY

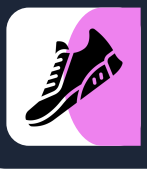
Online reselling communities, bots that snap up limited releases, and increased resale market activity have given these items speculative value, effectively turning them into alternative investments. In an economic environment facing uncertainty, consumers increasingly view hype items not as products to use, but as tangible assets with the potential to appreciate in value. This may offer a sense of financial control or potential returns that traditional savings may not provide.

In Q3, a key driver of economic uncertainty was the implementation of new US tariffs. In the Q1 QTR, Kasada IQ noted uncertainty around the impact of import tariffs. Several significant tariff policies have since been implemented, including a universal **10%** baseline on imports from almost all countries and a **55%** tariff on goods from China. While the White House indicated in September 2025 that tariffs could be lowered across industries, including food and pharmaceuticals, that is contingent on specific trade deals.

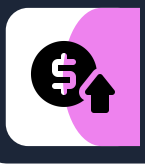
> Tariffs aren't the only driver of uncertainty. McKinsey reports top concerns for US consumers in the lead up to the 2025 holiday period are rising prices (**43%**), tariff policies (**29%**) and making ends meet (**22%**).
>
> **McKinsey**
> State of the Consumer 2025

Markets and their supply chains have responded. Retailers are hiking their prices, with some industries, like grocery, consumer goods and footwear, feeling it more than others. Key cogs in company-to-consumer supply chains are facing disruption.

In the US, the grocery component (referred to as food-at-home) of the Consumer Price Index rose **0.6%** in August 2025 and July 2025, the biggest month-to-month increase since August 2022.



The Yale Budget Lab estimated that tariffs will raise some categories of shoe as much as **39%** and some categories of apparel as much as **37%**. Prominent retailers, like Nike, increased shoe prices as it looks to reduce manufacturing in China.



Online retailers have passed extra costs associated with US tariffs to the consumer. Logistics suppliers servicing these online retailers charge a service fee equivalent to 10% of the tariff cost. Consumers also risk cancellations as some retailers will not ship to the US due to tariffs.

CASE SNAPSHOT: LOGISTICS OPERATIONS DISRUPTED BY TARIFFS

In August 2025, Australia Post temporarily suspended most parcel deliveries to the US due to changes in US tariff rules that removed the $800 de minis exemption. Prior to 26 August 2025, parcels getting shipped to the US that were under USD $800 were not taxed on arrival. The new tariff rules ended the de minimis exemption which allowed duty-free entry for packages in this category. The move effectively applied tariffs to nearly all imports. Australia Post subsequently indicated it will lift the suspension in October after partnering with a US Customs and Border Protection third party provider, Zonos, to process the required duties.

Several other postal services across Europe, Japan and Singapore have also suspended or restricted US-bound shipments while they figure out how to handle the new duties. For example, Singapore Post (SingPost) suspended some commercial shipments to the US in late August 2025 due to loss of the de minis exemption. SingPost then introduced Speedpost Direct International to handle shipments under USD $100, calculating all fees upfront to avoid customs surprises for customers.

Consumers are adapting their behaviors. Weaker consumer confidence and increased unemployment rates are expected to negatively impact consumption in the second half of 2025.

In August 2025, the unemployment rate in the US increased to nearly a four-year high of **4.3%**, with job growth slowing since April 2025.

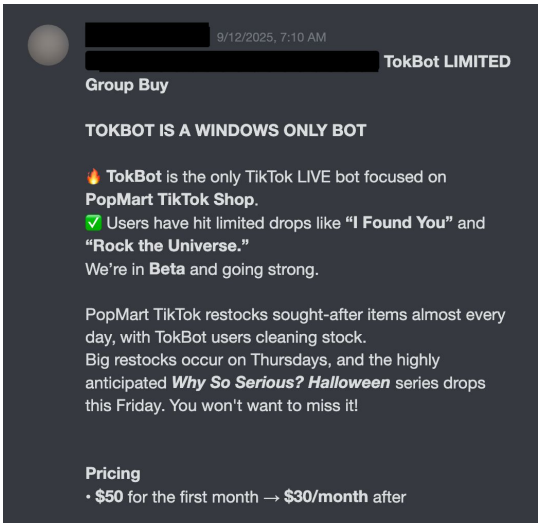
After sharply decreasing in April 2025 in both the US and Australia, consumer confidence has continued to fluctuate. Particularly in the US, consumer confidence in August 2025 was **6% lower** than January 2025, failing to recover to pre-tariff levels.

Overconsumption hits different for the younger generations. No cap. Consumers, particularly Gen Z, are reportedly demonstrating more risk-averse spending habits. With a large portion of members of online reselling communities falling into this generation, these insights are valuable in understanding the resurgence of automated reselling in 2025.

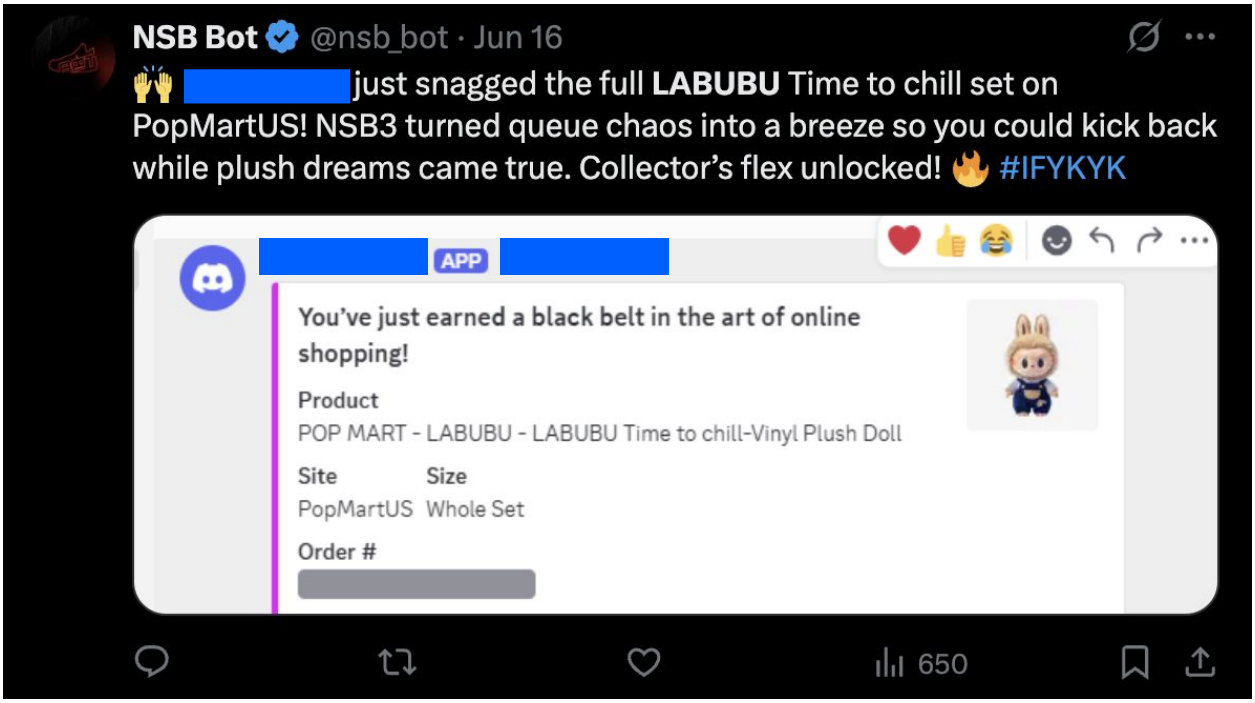
In September 2025, PwC reported that US consumers plan to cut spending during the upcoming holiday season, with Gen Z shoppers showing particularly frugal attitudes

Second-hand apparel retailer, ThredUp, reported that **64%** of younger generations consider resale value an important factor when purchasing new items, **36%** more than older generations in 2025.

Social commerce and social media platforms place a significant role in online reselling behaviour and engagement for younger generations. Kasada IQ has observed popular botting and reselling communities advertising specific bots for TikTok Shop and discussing ways to leverage TikTok Shop in their operations, as shown in the image. Sentiment within these communities indicates that while some claim they are able to get higher premiums on items they resell, others consider it difficult to scale and make good money on.



Community=Currency, Cultural Capital & FOMO. Online reselling leverages community as a form of currency and digital scarcity. Collecting and resale markets are now social activities driven by online forums, Discord, communities and social media. Platforms like these allow collectors to trade items and celebrate their finds. Rare collectibles are a form of social currency within these communities. Possessing a rare Labubu is a symbol of IYKYK (If You Know, You Know).



Brands are leveraging this by creating limited-edition drops and collaborations, driving a sense of FOMO (Fear of Missing Out). This sense of FOMO drives demand and increases the item's value in secondary markets. Researchers have compared collectible blind-box sales approaches to gambling, with scarcity driving irrational consumption behavior; a pattern that may signal broader issues with aspirational purchasing.

> Consumers invest more resources (cognitive and emotional) in pursuing uncertain rewards; this phenomenon parallels the psychobehavioral mechanisms observed in previous studies on lotteries and gambling
>
> **Xia, F., Xu, Y., Zhang, H. et al., 2025**
> The effect of doll blind box uncertainty on consumers' irrational consumption behavior: the role of instant gratification, Gambler's fallacy, and perceived scarcity

The Online Reselling Cycle

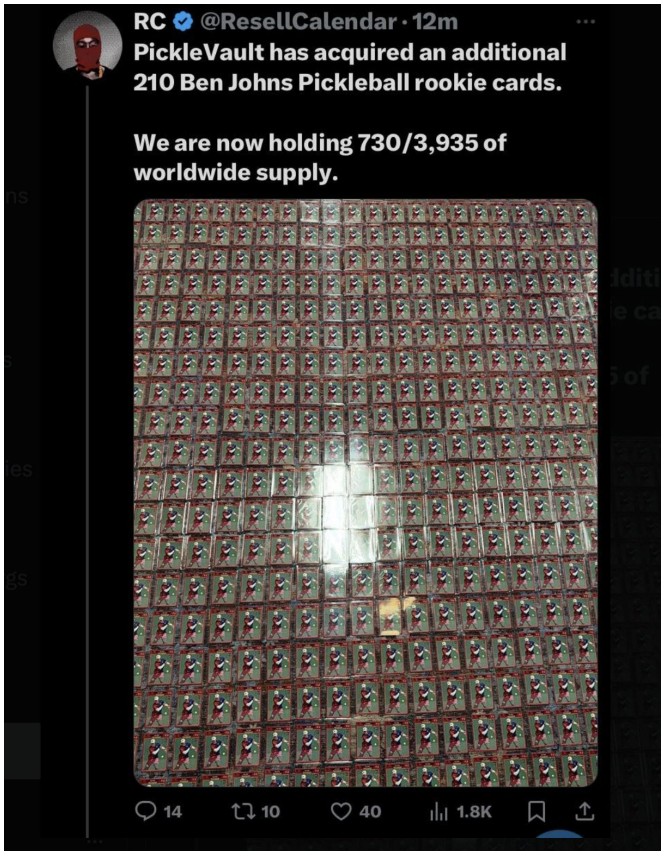
The online reselling community relies on the provision of bots and automated services by individuals or groups. Online reselling communities are often moderately sophisticated and organized, equipped to facilitate the buying and selling of high-demand, limited-edition products. The modus operandi for these adversaries is generally formulaic, as stepped out below.

Adversaries in this environment are generally males aged 18 to 30, though Kasada IQ has observed increasing involvement of individuals aged 30+. These individuals generally like to use social media and online communities to boast about their successes and profit, often positioning themselves as "influencers" in the "money-making" space. They tend to be heavily concentrated in the US.

01 IDENTIFY & TARGET PRODUCTS

Resellers target products characterized by extreme scarcity and high consumer demand, primarily sneakers and apparel, collectibles, and electronics. To identify profitable opportunities in these categories, resellers constantly scan the market using social media monitoring, trend analysis software, brand announcements, and resale calendars. However, hype is inherently cyclical. While some products maintain long-term value, Kasada IQ research shows that resellers typically shift focus to different hype items every 6 to 12 months, chasing the next wave of manufactured scarcity and following crowd behavior that amplifies demand spikes.

Resellers will also target products they can hoard stock to exacerbate scarcity so they can justify marking up their prices. While some resellers are part of communities, many who consider themselves "top-tier" will keep the sourcing methods and information secret to maintain their competitive edge. They may also engage in market manipulation, buying up all of a product' stock to artificially inflate the price and force buyers to purchase from them at a higher markup.



02 USE AUTOMATION TO GAIN AN ADVANTAGE

Resellers use automation to gain a competitive advantage by purchasing products much faster than any human can.

Sniper Bots	Place last-second bids on auction items. Sniper bots have features to give its users an advantage, including rapid price checking, price error monitoring, multiple wallets to spread bids across different auction items and floor price tracking.
Scalper Bots	Buy up large quantities of popular items and then resell them at a higher price.
All-In-One (AIO) Bots	Designed to work across a wide variety of eCommerce sites, automating the process of adding an item to a cart and checking out in milliseconds.
Proxy Networks	Resellers use proxy servers to hide their real IP addresses and make their bot traffic appear to be coming from a variety of different locations. This helps them to bypass a website's anti-bot measures and purchase multiple items.
Account Creation Bots	Resellers use these bots to automatically create thousands of fake accounts for a website or a raffle, which helps them to bypass a website's purchase limits and increase their chances of securing a product.

03 COMMUNITY-DRIVEN BUSINESS

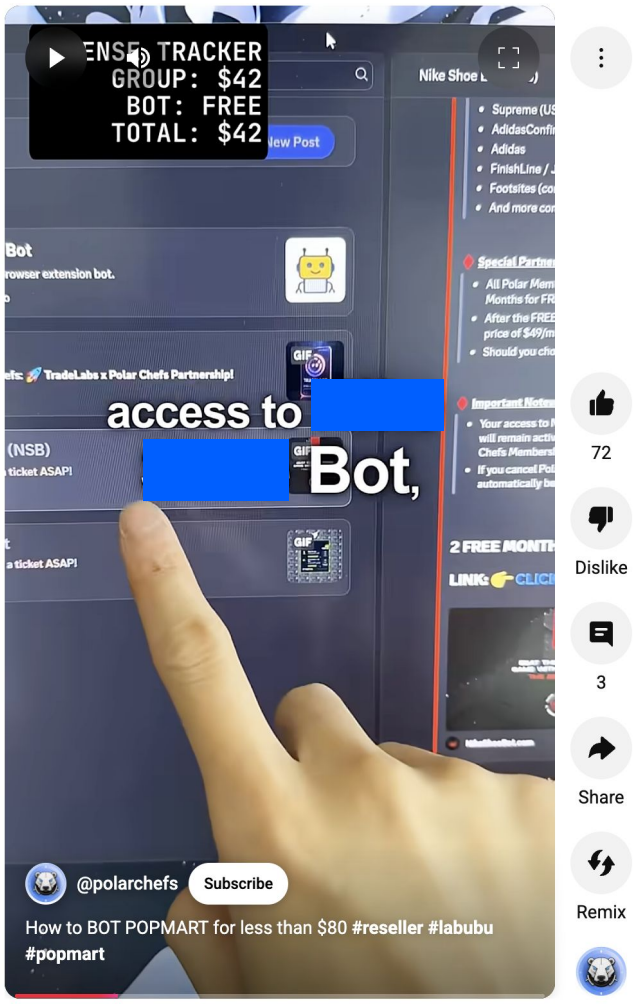
Community is core to the financial viability of online reselling operations. Even resellers who do not run their own community often rely on social media to boost their profile and advertise their inventory.

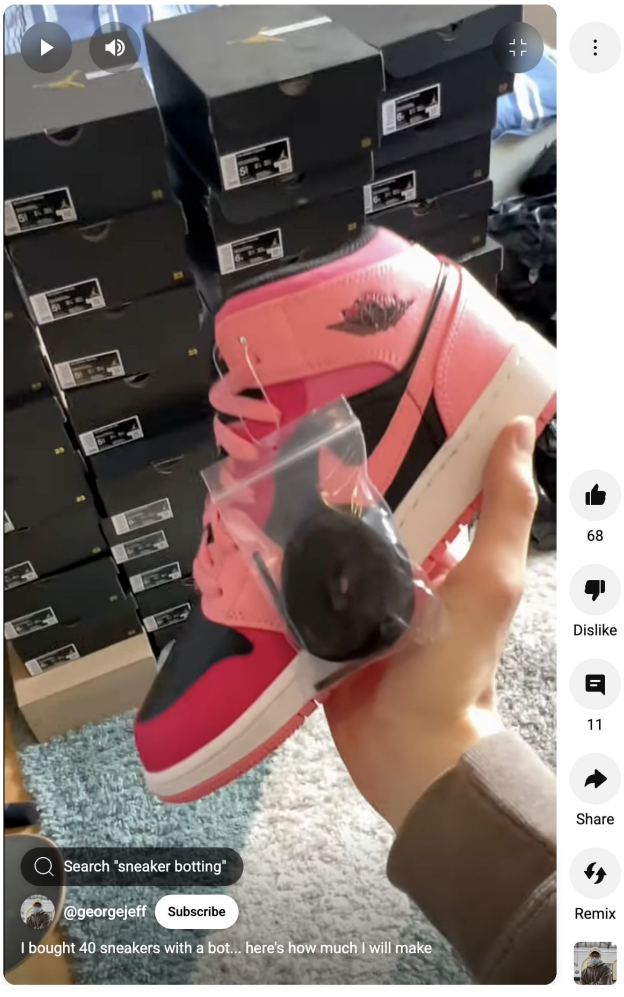
Resellers use the community to share intelligence (product drops, release dates, restocks) and sell resources (bots, proxies and accounts). Community is the core aspect in monetizing their operations, enabling them to sell products they acquire on the secondary market for significant markup.

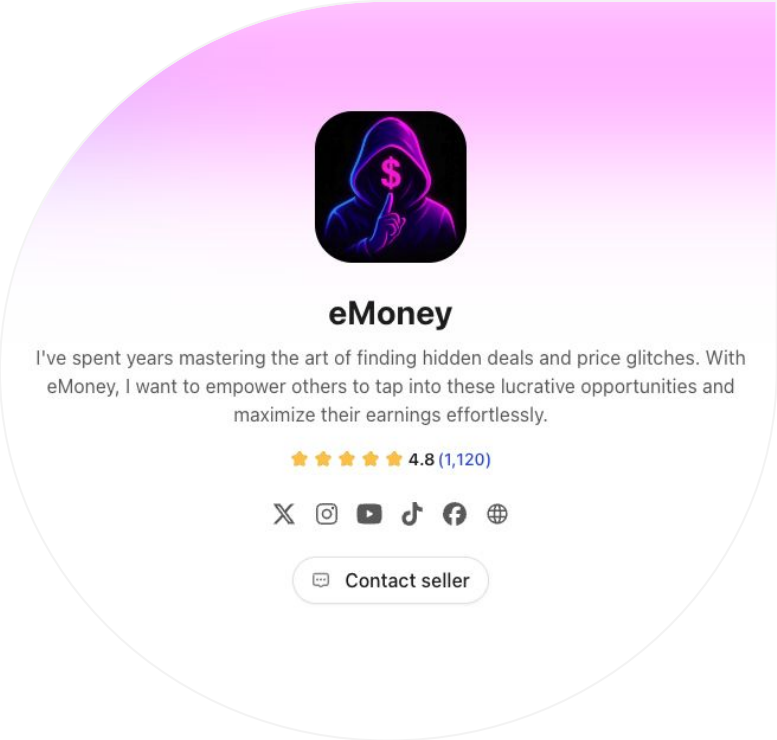
Community is often a function of personal branding for some resellers who boast their earnings and successes on social media. Several resellers present themselves as “mentors” or “influencers” who can help you “make money online” and be a “boss”. These kinds of resellers typically target an audience of young males. A large portion of this type of community engagement is personal branding and status, rather than trying to necessarily attract buyers to their operation.

How I “LEGALLY” Make $200,000/mo At 23 Years Old

Notably, Kasada IQ has observed some resellers on spec, meaning they are generating content to shop around their services or products in hope they will get paid. Rather than responding to a market demand, they are developing services and products and then attempting to generate demand and buyership through outreach. This outreach often comes in the form of short videos maximised to appeal to social media audiences.







ADVERSARY VIGNETTE:

EMONEY RESELLING

As reselling communities have ramped back up in 2025, Kasada IQ has observed an uptick in activity from some popular communities. One of these communities is eMoney, a Discord-based cook group (a group focused on buying limited items and reselling for profit). Advertising itself as the "#1 Reselling Community in the World", eMoney's primary focus is on reselling, price errors and glitches, clearance deals and flipping opportunities. Membership to eMoney's reselling community grew **140%** in August to September 2025.

FOSTERING, FLIPPING AND FAST CASH

Emerging in 2022, the US-based community was built by individuals who started out flipping (buying an item at a low price and quickly reselling for profit) who claim to have spent years perfecting the art. While they started small, eMoney's community has continued to grow in terms of membership, services and staff. It operates as a legitimate company, incorporated as FIREFLY FLIPS, LLC. It operates on Discord and Whop, with a public presence on most social media sites.

eMoney provides bots that scrape major stores and instantly notifies users of potential deals. Depending on the level of subscription, members can access automated tools and software. Some services, like the additional cost SeekerPro software, gives members access to clearance sales of up to 8 stores of their choosing. There is also specialised software for particular retails. Memberships for eMoney start at **USD $50**. In July 2025, eMoney stated its Premium Membership will increase from **USD $50 to USD $100** due to overwhelming demand.

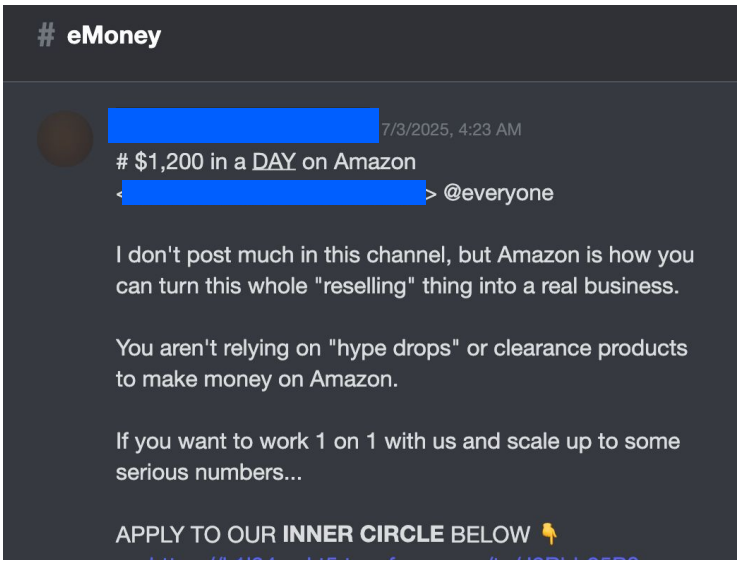
Kasada IQ estimates eMoney's monthly recurring revenue (MRR) to be at least **USD $275,000**. This estimate is based on membership to eMoney's paid server (accounting for around 18% for bots) and the lowest possible membership price. This is the floor not the ceiling, noting this data fluctuates and there are more expensive memberships.

eMoney prioritizes speed and volume over quality and hype. A large feature of eMoney's marketing approach is giving members the ability to find hidden deals or errors to then flip dozens of products over and over again. While a lot of eMoney's flipping activity is focused on low value items, like rubber brooms, eMoney also provides a platform for trading cards, like Pokemon and Topps, as well as ticket reselling. In Q3 2025, eMoney hosted webinars on ticket reselling and members boasted profits made from Ariana Grande tickets. Supported by customer testimonials, eMoney claims to make an extra USD $2,000 to $20,000 per month as per the below.

THE INNER CIRCLE

In March 2025, eMoney launched several Amazon programs which provide resources and mentorship at different levels starting from USD $50 a month. For USD $250 a month, eMoney offers access to its "Inner Circle" program, adopting a similar vernacular to the cryptocurrency community. The Inner Circle claims to reduce reliance on "hype drops" or clearance products to make large amounts of money, as picture on the right.

The Inner Circle guarantees results, involves hands-on coaching and gets members access to exclusive leads through sourcing partners. This plays on the status element of reselling communities, where selling more isn't just about profit.



Reselling Comes at a Cost

Reselling has come under fire in particular industries. In March 2025, the White House released an Executive Order (EO) on Combating Unfair Practices in the Live Entertainment Market. The EO noted that fans have paid as much as **70 times** the face value of a ticket price, with the additional profit going to scalpers and ticketing agencies.

Despite the *Better Online Ticket Sales (BOTS) Act* being in force since 2016, it has only been enforced once in 2021 against three New York-based ticket brokers. Since the EO, the Federal Trade Commission (FTC) has increased enforcement focus on both ticket brokers and major providers.

> Ticket scalpers use bots and other unfair means to acquire large quantities of face-value tickets and then resell them at an enormous markup on the secondary market.
>
> **White House Executive Order**
> March 2025

CASE SNAPSHOT: FTC V TICKET MARKET FRAUD

In Q3, the FTC launched two separate lawsuits against ticket broker operation, Key Investment Group (KIG) and affiliated companies and major entertainment provider, Ticketmaster. The FTC's allegations across both lawsuits is that the ticket market is a fraudulent and collusive environment, where deceptive practices (fake accounts, fake identities, proxies) are employed to harm consumers. The lawsuits send a clear message that the FTC is willing to target both the brokers who use the bots and the platforms that allegedly enable them

KIG allegations

The FTC alleged that KIG and its affiliated companies (Epic Seats, TotalTickets.com LLC, and Totally Tix LLC) bypassed Ticketmaster's protections, purchasing hundreds of thousands of tickets to resell at a significant markup. KIG allegedly purchased at least **379,776 tickets** in just over a year from Ticketmaster for nearly USD $57 million, reselling a portion for around **USD $64 million**. KIG allegedly used thousands of Ticketmaster accounts to purchase tickets, including fake and third party accounts, as well thousands of virtual and traditional credit card numbers. KIG used proxies, spoofed IP addresses and SIM boxes to disguise its activities.

Ticketmaster and Live Nation allegations

The FTC accused Ticketmaster and its parent company, Live Nation, of complicity. Ticketmaster and Live Nation allegedly were not just a victim of ticket brokers, but were actively aware of their illegal activities and coordinating with brokers. The FTC alleged that Ticketmaster engaged in deceptive practices, including claiming to impose strict limits on the number of tickets consumers could purchase for an event, despite ticket brokers routinely exceeding those limits. In an internal review, Ticketmaster found that just five brokers controlled **6,300+ Ticketmaster accounts** and had **246,000+ tickets** to **2,500+ events** in their possession.

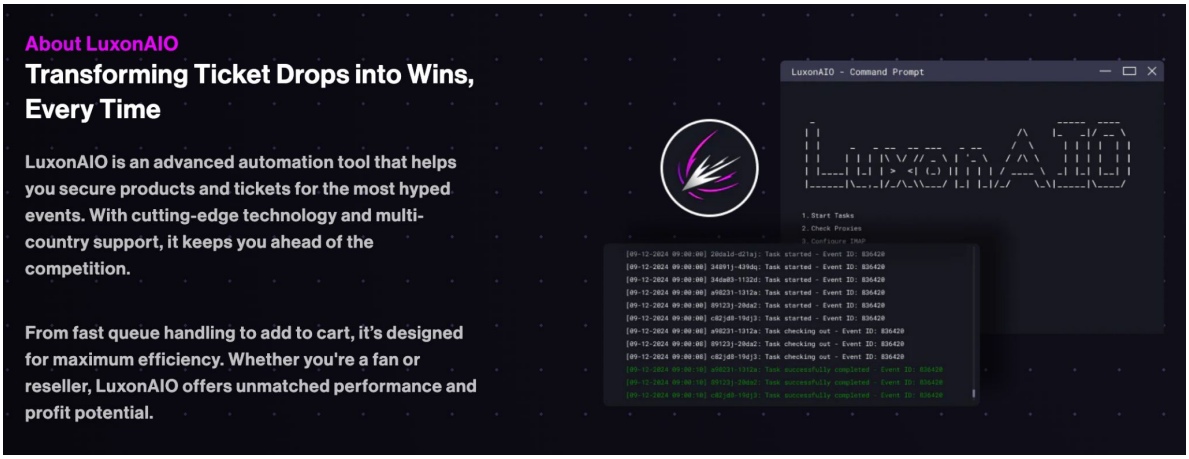
A CONTEMPORARY CHALLENGE

In September, there was significant public backlash about Ariana Grande's 2026 tour presale tickets selling out within minutes on Ticketmaster. Notably, Ariana Grande tickets were not dynamically priced in the interest of consumers. It appears that fixed pricing primarily benefited ticket scalpers who bought up stock to resell at significant markup.

Dynamic pricing involves **adjusting prices in real-time** in response to factors like market demand, supply changes, competitor pricing and consumer behavior.

On platforms like StubHub and Viagogo, tickets to some Ariana Grande shows in the US are being sold for **USD $9,000+**. Members of some online reselling communities are boasting about the profits they have made from reselling Ariana Grande tickets, relying on the automated services provided to them by the operator.

This kind of activity is not new. Kasada previously uncovered multiple groups of up to 500 resellers conducting an active operation to buy 18,000+ tickets for a popular event and resell them for profit. A conservative estimate of this operation indicated resellers were making over **USD $1 million** in profit. Scalper bots use automated methods to obtain goods or services, which they can buy in bulk and finish the checkout process at a speed no human can compete with. Scalpers will purchase tickets in bulk then upload them to popular ticket reselling marketplaces of classified sites, like StubHub and Viagogo. Depending on the ticket price and the event itself, these entry passes can be sold at multiple times their face value. Kasada IQ has observed several bots specifically developed to target Ticketmaster in specific regions, like LuxonAIO's offering in the image below.



While the activity is not new, attitudes are changing. With consumers, media and government calling out ticketing companies and resellers and increasingly pursuing legal action. As a result, bot developers must operate with heightened risk and deploy more sophisticated evasion tactics. The ticketing industry and the parallel scalping industry are likely to face continued, heightened scrutiny from law enforcement and consumers.

Impacts for Businesses

Loyal customers are at a disadvantage when coming against automated reselling communities. When a highly anticipated product sells out to bots, the average customer feels unfairly cheated, leading to frustration and anger towards the brand. With this at its core, businesses can face a loss of brand control. With online reselling communities taking charge, the brand is no longer setting the price or defining the product value. Whether true or not, it can send a message that the business is not managing its own sales and its products are being controlled by secondary forces. While scarcity creates hype, when the hype is fueled by bots and not genuine consumer demand, it can backfire.

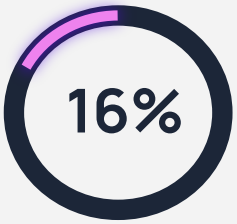
Consumers value a relationship with the brand. When a bot buys a product, the business loses that opportunity for customer connection. This translates to a loss of valuable customer data, customer relations and brand loyalty. The customer becomes an anonymous transaction, which holds little long-term value. Bot activity also often involves the creation of high volumes of fake accounts with incomplete or fabricated information. This data can pollute customer databases, making it harder to analyze behavior, run effective marketing campaigns and maintain security.

Bots can create artificial demand for products, leading a business to misjudge its inventory and future sales. A business may see a product sell out in seconds and believe there is higher demand for it than there actually is, leading to an oversupply in future. Keeping up with these bots and online reselling communities can be tedious and demanding for businesses self-managing the threat. The botting ecosystem is constantly evolving, with adversaries adopting new technologies and methodologies to stay operational and competitive. Businesses need to continually invest in new security measures, anti-bot software and fraud detection tools.

Threat Landscape Update

TOP THREAT

Account Takeover (ATO) remained the **top threat** tracked by Kasada IQ in Q3. The targeted industries shifted in Q3, reflecting how adversaries are pivoting to where demand was highest and defenses weakest.



Increase in observed account sales in Q3

Top Industries for Account Sales:

- Retail
- Quick Service Restaurants
- Webmail

See **Account Takeover (ATO)** for more detail.

ATTACK INTENT

The top intent classifications for attempted attacks were in Q3 were:

API Automation

Account Takeover

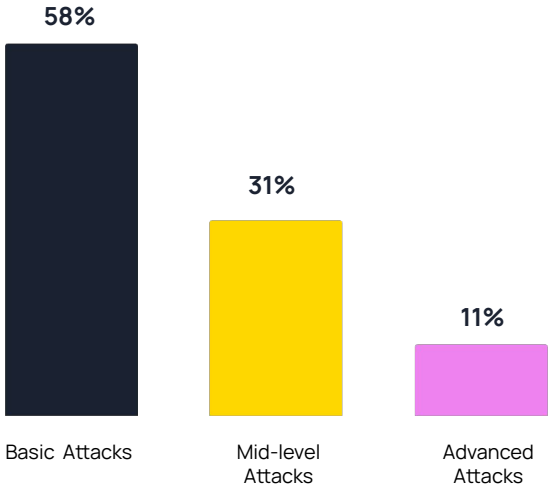
Checkout Fraud

Content Scraping

Fake Account Creation

BOT SOPHISTICATION

Consistent with Q1 and Q2, the majority of attacks observed by Kasada were assessed as basic. We note that basic does not equate to low impact, with basic bot activity often scalable and overlooked.



Analyst Commentary

ACCOUNT THEFT VECTORS

Several industry resources reported on attack vectors for account theft to harvest credentials at scale, including novel and existing information stealers (infostealers). This included the open-source Stealerium malware, the python-based PXA Stealer and the VBS Cmimai Stealer. Notably, the prolific Lumma Sealer Malware-as-a-Service resumed operations after a law enforcement takedown of its infrastructure in May 2025. From June to July 2025, the number of targeted accounts surged. Recorded Future provided in-depth analysis on the Lumma Stealer operation.

In looking at novel vectors, Bitdefender reported that adversaries are using browser extensions claiming to unlock the blue verification tick on Facebook and other features to steal Meta accounts, including some Facebook Business accounts. ReliaQuest reported that adversaries are increasingly exploiting the Axios user agent to automate phishing and credential theft at unprecedented scale. Axios enables adversaries to juggle tasks like sending HTTP requests, stealing credentials, and hitting APIs simultaneously. ReliaQuest reported that Axios user agent activity surged **241%** from June to August 2025, dwarfing all other flagged user agents combined (**85%**). Cofense observed a significant increase in the abuse of the `.es` top level domain (TLD) for malicious activity in the first half of 2025. From Q4 2024 to Q1 2025, `.es` TLD abuse increased 19x and became part of the top 10 abused TLDs in credential phishing. `.es` TLD domains now appear about 2x more often than `.dev` in malicious campaigns. There were no unique patterns in campaigns using `.es` TLD domains, indicating that abuse of `.es` TLD domains is becoming a common technique among a large group of adversaries.

ANALYST COMMENT I In Q3, adversaries continued to show a clear preference for proven methods. The infostealer ecosystem continues to demonstrate resilience, with disruptions of infrastructure only temporary setbacks for well-established operations. The continued proliferation of infostealers, including open-source and python variants, highlights the credentials remain a highly profitable and accessible target for cybercriminals. Emerging vectors, like the Axios user agent and malicious browser extensions, are designed to bypass traditional security defenses that rely on signature-based detection. These developments emphasise the need to maintain traditional defenses, but enhance with behavioral and AI-based detection.

OBFUSCATION IS ENABLING ENABLERS

Recorded Future reported that web hosting provider, Stark Industries Solutions Ltd (Stark), made a series of infrastructure and organisational changes to evade sanctions and preserve operational continuity. Stark rebranded as THE.Hosting under the control of Dutch entity, WorkTitans B.V. Stark was sanctioned for enabling state-sponsored cyber operations linked to Russia, Iran, North Korea and China, as well as cybercriminals. Separately, researchers identified and linked three families of seemingly distinct VPN providers which collectively account for over 700 million downloads on the Google Play Store. The researchers found that many of the providers, which claim to be in places like Singapore, are actually owned by a single entity and collect location data despite explicitly stating they do not.

ANALYST COMMENT I These developments demonstrate how active enablers of threats, such as infrastructure providers, use sophisticated, deceptive business practices to remain operational. Active enablers are well-positioned to rebrand, reallocate infrastructure and maintain operational continuity. These kinds of enablers are structurally resilient, demonstrating the need to go beyond defensive monitoring and engage in proactive, bespoke defenses. Further, these findings demonstrate that enablers are fundamentally undermining the security and privacy they claim to provide.

PROXY NETWORKS OPERATING FROM YOUR HOME

Infrawatch reported on Belarus-linked residential proxy network, DSLroot, uniquely deploying dedicated hardware (like. laptops) inside US residences to create persistent, managed access to US home networks. The hardware setup allows the operator to remotely control the devices, force IP address rotation and route client traffic anonymously through the compromised residential IPs. DSLRoot's services also include virtual credit card issuance and are advertised on forums like BlackHatWorld.

ANALYST COMMENT I In the Q2 QTR, Kasada IQ reported on residential proxy network providers embedding software development kits (SDKs) into freemium apps, transforming end-user devices into residential proxies without explicit user awareness. DSLRoot represents a different approach to the same end goal. Instead of hiding proxy software in apps, DSLRoot openly recruits users by paying them to share their internet connection and providing them hardware to do so. The provided hardware operates as a proxy node, earning the user a passive income in exchange for their bandwidth. Both models represent a shift toward proxy networks built not through malware, but through user consent, termed as "legal botnets". This consent could be buried in Terms of Service agreements or provided explicitly, as was the case with DSLRoot users.

The quality of that consent is highly questionable. As security journalist Brian Krebs reported, many DSLRoot users don't understand they're becoming exit nodes for potentially malicious traffic. While SDKs get people to monetize unused bandwidth, DSLRoot gives its users access to connections if they agree to share your own. One self-described US Air National Guard member stated on Reddit that they had signed up as a "naïve 18 year old" and continued for 5 to 6 years without understanding the true nature of the service or the security implications. These "legal botnets" pose unique detection challenges for traditional security tools. Unlike malware-based proxy networks, the software is digitally signed, willingly installed by users, and operates with ostensible permission, making it difficult to classify as malicious despite the risks it creates.

AI Updates

Throughout Q3, adversaries continued to find new and improved ways to use AI to their advantage. Adversaries are using AI in every stage of their campaigns, finding creative ways to enhance operational security, speed up their operations and scale their attacks. In limited instances, adversaries have used the threat of AI itself as a tool in attacks against businesses. As markets adapt to an increasingly AI-driven landscape, the opportunities for adversaries are increasing.

ACTIVE THREATS

Anthropic's Threat Intelligence Report: August 2025 reported that agentic AI systems are being weaponized. Cybercriminals are embedding AI throughout their operations, with AI being used for all stages of fraud operations. Amongst other threats, adversaries were observed using AI to enhance and scale their operations. This included using Claude to analyze stealer logs, process stolen cards and build victim profiles.

ANALYST COMMENT | Anthropic's report provides tangible insights into how adversaries are using AI to scale and supplement parts of their operations. By using AI, an adversary can achieve the impact of an entire criminal operation. Across all operations uncovered by Anthropic, resilience was a large component. AI facilitates quick pivots and adaptations when facing blocks or detection. This makes defense increasingly difficult, with AI-generated attacks adapting to defensive measures in real-time. These shifts demonstrate a need for new frameworks for evaluating cyber threats that consider AI-enabled attacks. With AI providing instant access to expertise, traditional assumptions about adversary capability and attack sophistication are no longer valid.

THREAT ENABLERS

Proton launched its privacy-focussed AI assistant, Lumo, which prevents third parties from accessing content. Proton grants users an encryption key that only they can use to view their content, ensuring that Proton cannot share user data with advertisers or governments, or use it to train LLMs. Lumo includes a "Ghost mode" that makes your conversation disappear forever when you close it. Users can also link Proton Drive files to Lumo and everything stays encrypted. Its base service is free to use, making it widely accessible.

ANALYST COMMENT I Adversaries could believe that using the "privacy-focused" Lumo grants them anonymity for illicit activities. This is similar to how adversaries have used the encrypted email service, Proton Mail. Adversaries have used Proton Mail to coordinate illicit activities, often used by individuals operating on the dark web for communications related to criminal marketplaces and hacking forums. Proton Mail is also commonly used for spam and phishing campaigns, as well as fake account creation. We attempted to ask questions of Lumo around nefarious activities, like "how can I hack an account?", and Lumo failed to respond. Despite not mentioning any terms of use, it appears to block obviously malicious content.

OPPORTUNITIES

Delta Airlines' use of generative AI to price some flights has been subject to scrutiny from US senators who have labelled it "predatory" or "surveillance" pricing. Delta's AI uses a continuous pricing model that uses context clues (market-level demand, time of day, how far in advance, competitor pricing) to set a fare for a specific customer. In partnership with Israeli AI pricing company, Fetcherr, Delta is aiming to increase usage of this kind of pricing from 3% to 20% by the end of 2025.

ANALYST COMMENT I Adversaries could abuse AI pricing systems for financial gain or to manipulate the market to gain a competitive advantage. An adversary could generate phantom demand for a product or flight by generating bulk fake searches.They could also feed false, low prices for a competitor's product into a system which could influence the AI to drop its own prices to remain competitive. There are many potential avenues that adversaries could take to manipulate this kind of pricing approach, many of which could lead to significant revenue loss for businesses employing it.

INDUSTRY IMPACTS

MEDIA AND CONTENT

In September, Anthropic agreed to pay at least USD $1.5 billion to settle a class action lawsuit brought by authors and publishers (*Bartz et al. v. Anthropic PBC*). The class action argued that Anthropic illegally used pirated books to train its AI model, Claude. The judge held that while using copyrighted materials to train an AI model might be considered "fair use", the act of acquiring and retaining a library of books from pirate websites is not. This means indiscriminate scraping of websites poses additional legal risks for AI companies.

Subsequently, major brands, including Reddit, announced support for a new licensing standard, Really Simple Licensing (RSL). RSL aims to let web publishers set terms of how AI system developers use their work and how they should pay to scrape their sites. The RSL Standard directly addresses the piracy problem by enabling AI companies to license content directly from creators and publishers but remains under development. It is based on the widely adopted Really Simple Syndication (RSS) standard that scales to millions of websites and can be applied to any digital content and datasets. The RSL standard builds upon the robots.txt protocol, but goes further by adding licensing and royalty terms to their robots.txt file. They can also embed terms in online books, videos and training datasets they may want compensation for. The RSL Standard supports several licensing models, including subscription fees, pay-per-crawl fees or free ones.

ANALYST COMMENT I The RSL Collective believe it will be legally enforceable, likening it to music rights organisations like the American Society of Composers, Authors and Publishers (ASCAP) and Broadcast Music, Inc. (BMI). ASCAP and BMI collect and distribute royalties for musical compositions when they are publicly performed, like on radio. However, the RSL still heavily relies on the cooperation of and adoption by AI companies. AI companies already ignore robots.txt and the standard alone cannot block AI crawlers or other forms of bots. The RSL Collective is working with Content Delivery Network (CDN) provider, Fastly, to admit bots to websites based on whether they have agreed to license content. Once developed, this could act as a "gatekeeper". In the long-term, new data brokers could emerge, with companies specialising in aggregating and licensing RSL-compliant data. As companies would move to paying for data, there could be heightened demand for quality. This could lead to a market that favours curated, authoritative datasets over indiscriminate web scraping.

Throughout Q3, legal challenges against AI companies, predominantly from media-related industries, significantly increased. While the sentiment behind the RSL Standard and similar initiatives canvassed before is not necessarily new, AI companies are facing an unprecedented amount of legal and public scrutiny which could influence more buy-in to the RSL Standard.

INDUSTRY IMPACTS

RETAIL & ECOMMERCE

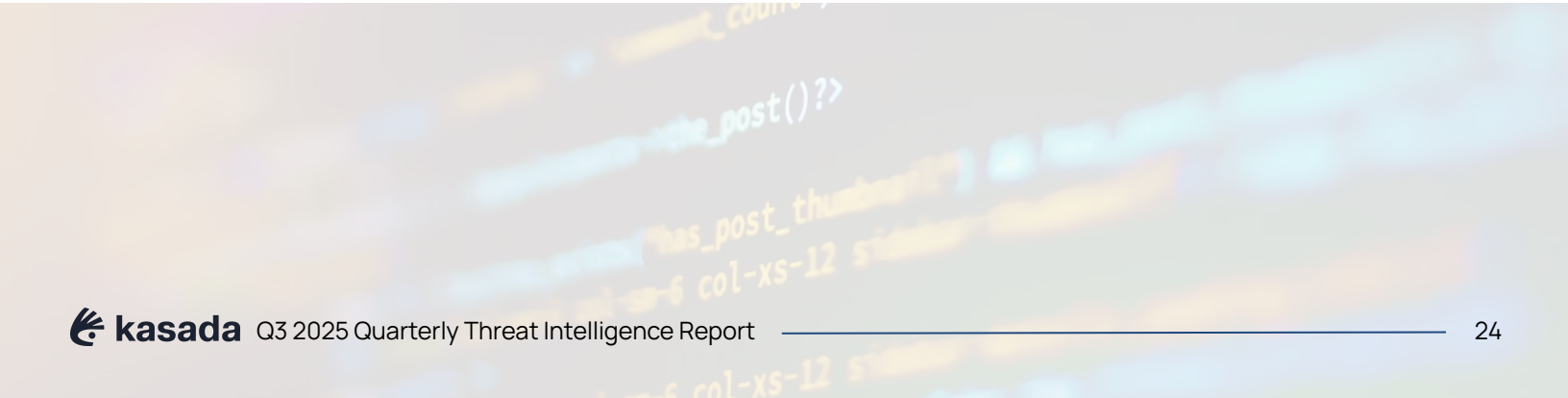
In Q3, the rapid emergence of AI web browsers marked a major shift in the landscape. Several AI-native developers, like Perplexity and Claude, launched agentic browsers designed to perform multi-step tasks. Tasks include booking meetings, comparing prices and making transactions. Several major players in the industry subsequently integrated their large language models (LLMs) into core browsers.

Despite this large-scale rollout, several researchers have identified serious security deficits. Guardio described this new landscape with the term "Scamlexity", where existing tricks hit harder and new AI-born attack vectors continually surface. Through building and testing three scenarios, Guardio was able to demonstrate the following:

- An AI browser can be instructed to buy merchandise from a fake retail website. The AI autonomously navigated the site, added the product to card and auto-filled saved credit card information.
- An AI browser can treat obviously malicious emails as legitimate and click on malicious links.
- Follow hidden instructions in fake CAPTCHAs without the user's knowledge resulting in drive-by-downloads of malicious files.

ANALYST COMMENT I This development demonstrates how adversaries don't need to rely on fooling a human. With AI browsers they can bypass the human completely and use the AI as an extension of their attack chain. This development occurs alongside reporting from Forbes which claims that AI browsers and assistants (ChatGPT, Claude, Perplexity) are driving eCommerce traffic away from Amazon and reducing the relevance of Google Search. Adobe also reported that Gen-AI driven traffic to US eCommerce sites is up 4,700% in H1 2025. Revenue from AI-driven traffic also increased by 84% in the same time period. This means two things:

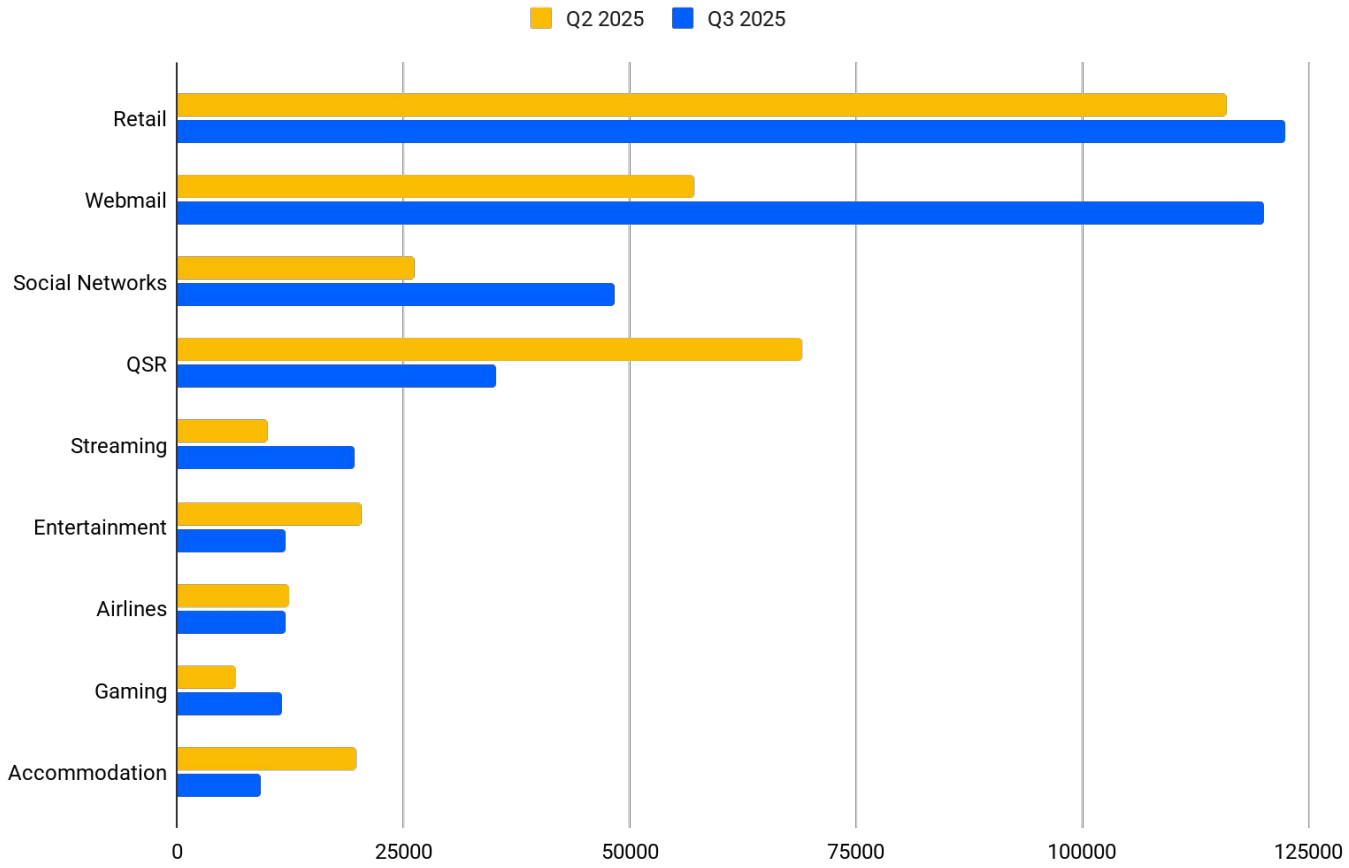
1. Businesses are being driven to invest and ensure their data is captured by AI. The normal things common for SEO (keywords, backlinks and blogspam) aren't captured by AI assistants. The AI relies on Q&A-rich structured data that helps add context to answers. To stay competitive, eCommerce businesses are encouraged to shift to Generative Engine Optimization (GEO). This further pushes the uptake of AI over classic search engines.
2. More people using AI browsers and assistants significantly expands the attack surface for adversaries.



Account Takeover (ATO)

ATO remained the **top threat** tracked by Kasada IQ in Q3. In Q3, the underground market for stolen accounts continued to evolve, with total observed account sales rising to about **390,000** – an increase of roughly **16%** from Q2.

The targeted industries shifted in Q3. In Q2, **retail, quick service restaurants (QSRs) and webmail** were the top three sectors, comprising **~72%** of all stolen account sales. In Q3, retail and webmail remained dominant but social network accounts surged into the top 3, displacing QSR. This reflects cybercriminals pivoting to where demand was highest and defenses weakest.



ACCOUNT SALES BY INDUSTRY

In Q3, growth was uneven across industries. As shown below, **webmail**, **social networking**, **streaming**, and **gaming** accounts saw dramatic spikes in sales volume, while **accommodation**, **QSRs**, and **entertainment & ticketing** accounts experienced steep declines compared to Q2. Retail account sales edged up modestly, and airline accounts held roughly steady quarter-on-quarter (QoQ).

Industry	Total Sales	Stores Selling Accounts	Maximum Available Stock	Revenue from Sales	Average Account Price
Accommodation	9,186▼	62▼	58,951▼	$81,390▼	$8.86▲
Airlines	12,008▼	82▲	96,742▼	$184,882▼	$15.35▼
Entertainment & Ticketing	12,038▼	107▼	127,620▲	$26,781▼	$2.16▼
Gaming	11,609▲	330▼	407,636▼	$28,725▲	$2.47▲
Quick Service Restaurants	35,146▼	227▼	404,582▼	$74,219▼	$2.43▲
Retail	123,494▲	556▼	802,277▼	$546,751▲	$3.47▲
Social Networks	48,352▲	383▲	198,434▲	$39,103▲	$0.81▲
Streaming	19,647▲	769▼	644,747▲	$116,346▲	$5.92▲
Webmail	120,070▲	226▲	300,611▼	$67,485▼	$0.56▼

As previously mentioned, social networks bumped QSRs out of the top three industries for observed account sales, sitting alongside retail and webmail. Notably, the total number of webmail accounts sold more than doubled QoQ (to 120,070 in Q3 from 57,176 in Q2), making webmail one of the largest categories by volume. Social media logins jumped even more (up **~84%** QoQ), while streaming service accounts nearly doubled as well. Meanwhile, hospitality and food service accounts saw significant drops after a strong Q2, suggesting a seasonal and situational ebb in criminal activity for those sectors.

Several factors help explain these shifts: seasonal behaviors (such as summer travel season winding down, back-to-school period, pre-holiday lulls), major events and releases (in gaming and entertainment), changes in consumer habits (such as responses to password-sharing crackdowns), and cybercriminal tactics (such as exploiting new breaches or shifting to more lucrative targets).

The massive availability of stolen credentials in 2025 cannot be overstated. Over 1.8 billion credentials were compromised in the first half of 2025, an 800% increase year-on-year. This has supercharged the supply available to criminal marketplaces.

ACCOMODATION

Accommodation accounts fell sharply QoQ: 9,186 sold (**-53.7%** vs 19,859 in Q2), $81,390 revenue (**-50.4%** vs $164,170), and average price $8.86 (**+7.1%** vs $8.27). Seller count edged down to 62 (**-4.6%** vs 65) while available stock more than halved to 58,951 (**-44.5%** vs 106,187).

The pattern mirrors post-peak seasonality: after Q2's spring planning surge, fewer travelers sought (or could monetize) hijacked loyalty accounts in late summer, while hospitality firms appear to have tightened controls and cleaned up compromised balances. That said, pricing held firm; a sign that the listings that did sell skewed toward high-value loyalty profiles (points/elite status).

54% ▼
Account Sales

50% ▼
Revenue

5% ▼
Active Shops

44% ▼
Total Stock

AIRLINES

Sales held near flat at 12,008 (**-2.0%** vs 12,252), but revenue slid to $184,882 (**-32.5%** vs $273,938) as the average price dropped to $15.35 (**-31.4%** vs $22.36). Stores ticked up to 82 (**+1.2%** vs 81), while stock declined to 96,742 (**-17.6%** vs 117,420).

This price compression aligns with Q3 airline breach headlines that flooded markets with travel logins/miles and depressed prices: in early July, Qantas disclosed a breach of up to 6 million customers (names, contact details, DOBs, and frequent-flyer numbers via a third-party platform), followed by WestJet confirming 1.2 million customers were affected in a June 2025 breach. With more sellers but less stock and lower Average Revenue Per User (ARPU), Q3's data suggest an oversupply of middling-quality accounts and tougher monetization as airlines expand MFA/monitoring of loyalty abuse.

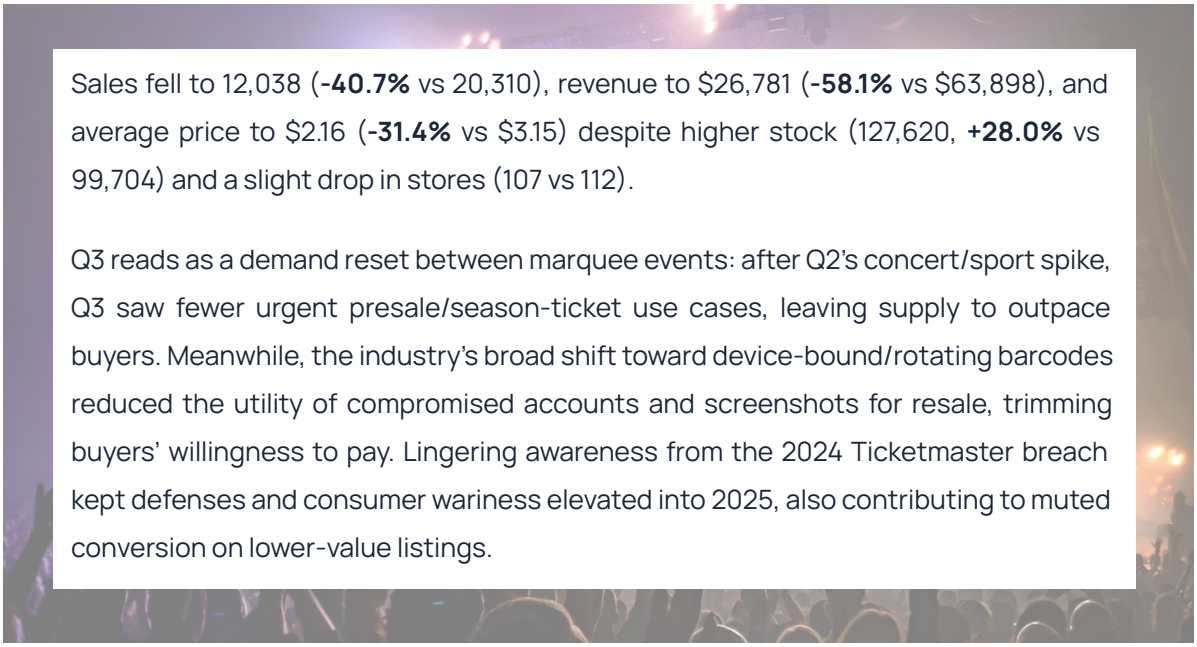
2% ▼
Account Sales

33% ▼
Revenue

1% ▲
Active Shops

18% ▼
Total Stock

ENTERTAINMENT & TICKETING



Sales fell to 12,038 (**-40.7%** vs 20,310), revenue to $26,781 (**-58.1%** vs $63,898), and average price to $2.16 (**-31.4%** vs $3.15) despite higher stock (127,620, **+28.0%** vs 99,704) and a slight drop in stores (107 vs 112).

Q3 reads as a demand reset between marquee events: after Q2's concert/sport spike, Q3 saw fewer urgent presale/season-ticket use cases, leaving supply to outpace buyers. Meanwhile, the industry's broad shift toward device-bound/rotating barcodes reduced the utility of compromised accounts and screenshots for resale, trimming buyers' willingness to pay. Lingering awareness from the 2024 Ticketmaster breach kept defenses and consumer wariness elevated into 2025, also contributing to muted conversion on lower-value listings.

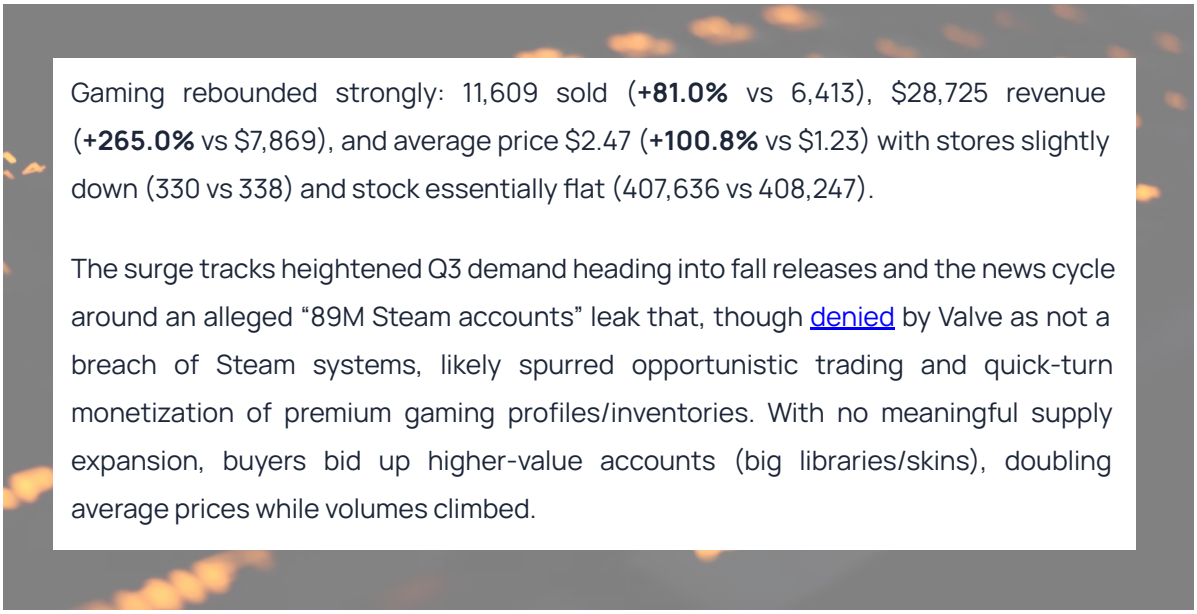
41% ▼
Account Sales

58% ▼
Revenue

4% ▼
Active Shops

28% ▲
Total Stock

GAMING



Gaming rebounded strongly: 11,609 sold (**+81.0%** vs 6,413), $28,725 revenue (**+265.0%** vs $7,869), and average price $2.47 (**+100.8%** vs $1.23) with stores slightly down (330 vs 338) and stock essentially flat (407,636 vs 408,247).

The surge tracks heightened Q3 demand heading into fall releases and the news cycle around an alleged "89M Steam accounts" leak that, though denied by Valve as not a breach of Steam systems, likely spurred opportunistic trading and quick-turn monetization of premium gaming profiles/inventories. With no meaningful supply expansion, buyers bid up higher-value accounts (big libraries/skins), doubling average prices while volumes climbed.

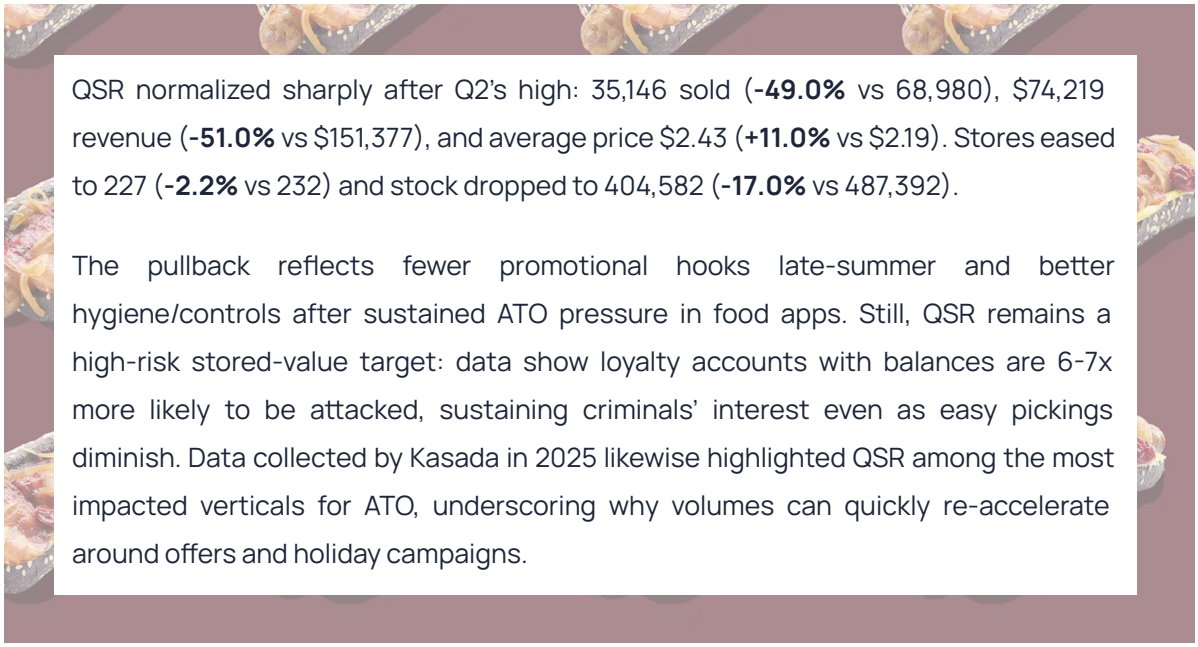
81% ▲
Account Sales

265% ▲
Revenue

2% ▼
Active Shops

0.2% ▼
Total Stock

QUICK SERVICE RESTAURANTS (QSR)



QSR normalized sharply after Q2's high: 35,146 sold (**-49.0%** vs 68,980), $74,219 revenue (**-51.0%** vs $151,377), and average price $2.43 (**+11.0%** vs $2.19). Stores eased to 227 (**-2.2%** vs 232) and stock dropped to 404,582 (**-17.0%** vs 487,392).

The pullback reflects fewer promotional hooks late-summer and better hygiene/controls after sustained ATO pressure in food apps. Still, QSR remains a high-risk stored-value target: data show loyalty accounts with balances are 6-7x more likely to be attacked, sustaining criminals' interest even as easy pickings diminish. Data collected by Kasada in 2025 likewise highlighted QSR among the most impacted verticals for ATO, underscoring why volumes can quickly re-accelerate around offers and holiday campaigns.

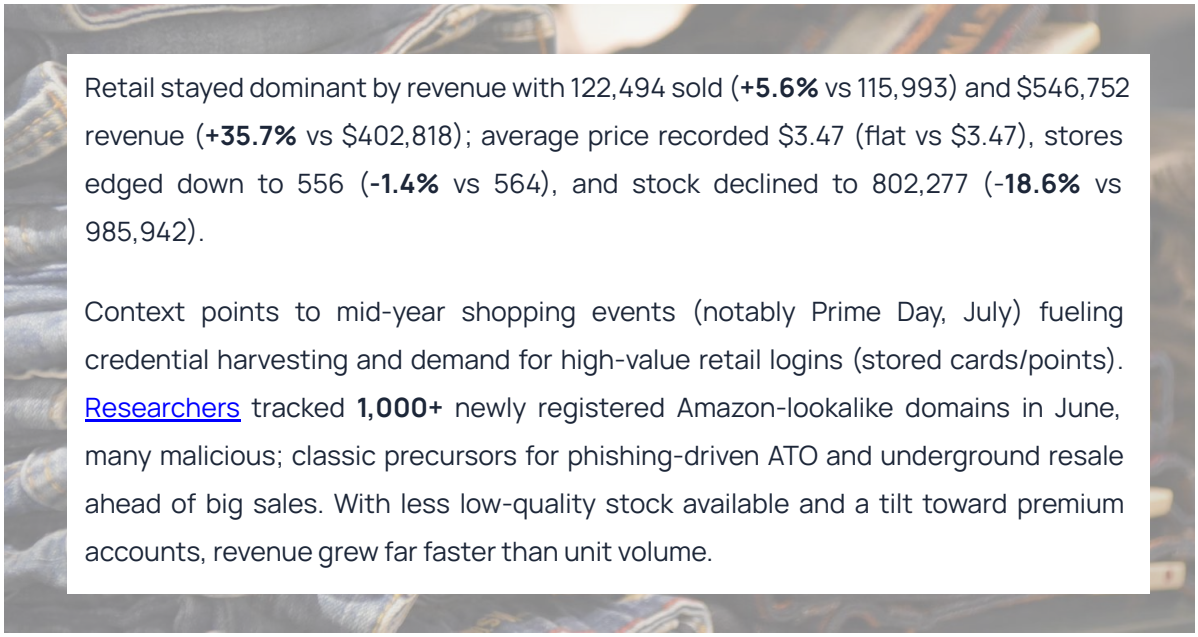
49% ▼
Account Sales

51% ▼
Revenue

2% ▼
Active Shops

17% ▼
Total Stock

RETAIL



Retail stayed dominant by revenue with 122,494 sold (**+5.6%** vs 115,993) and $546,752 revenue (**+35.7%** vs $402,818); average price recorded $3.47 (flat vs $3.47), stores edged down to 556 (**-1.4%** vs 564), and stock declined to 802,277 (-**18.6%** vs 985,942).

Context points to mid-year shopping events (notably Prime Day, July) fueling credential harvesting and demand for high-value retail logins (stored cards/points). Researchers tracked **1,000+** newly registered Amazon-lookalike domains in June, many malicious; classic precursors for phishing-driven ATO and underground resale ahead of big sales. With less low-quality stock available and a tilt toward premium accounts, revenue grew far faster than unit volume.

6% ▲
Account Sales

36% ▲
Revenue

1% ▼
Active Shops

19% ▼
Total Stock

SOCIAL NETWORKS

Social accounts surged: 48,352 sold (**+83.9%** vs 26,292), $39,103 revenue (**+155.3%** vs $15,319), and average price $0.81 (**+39.7%** vs $0.58). Stores rose to 383 (**+1.9%** vs 376) while stock fell to 198,434 (**-31.9%** vs 291,482).

The price and volume lift, alongside shrinking stock, signals strong demand for aged/influencer handles used in large-scale scams. Researchers documented the continued abuse of hijacked channels for "stream-jacking" crypto scams and malware, with thousands of malicious livestreams on popular platforms and high-follower accounts repeatedly targeted. Q3 data aligns with that pressure: buyers pay more for trusted-looking identities that deliver reach and evasion.

84% ▲
Account Sales

155% ▲
Revenue

2% ▲
Active Shops

32% ▼
Total Stock

STREAMING

Streaming saw near-doubling in unit sales: 19,647 sold (**+95.8%** vs 10,033) and $116,346 revenue (**+4.4%** vs $111,455), with average price $5.92 (**+272%** vs $1.59), stores at 769 (**-1.0%** vs 777), and stock up to 644,747 (**+5.9%** vs 608,785).

The volume-at-scale model continued: password-sharing crackdowns nudged some consumers toward illicit, low-cost access, which Kasada has tracked since 2023 (such as dark-web Netflix accounts offered for just a few dollars), keeping underground unit prices attractive even as platforms tighten access rules. The net effect in Q3: many more accounts moved, modest revenue growth, and a higher realized price on average compared to the prior quarter's recorded figure; reflecting bulk buyers paying a bit more for longer-lived access amid device checks and login frictions.

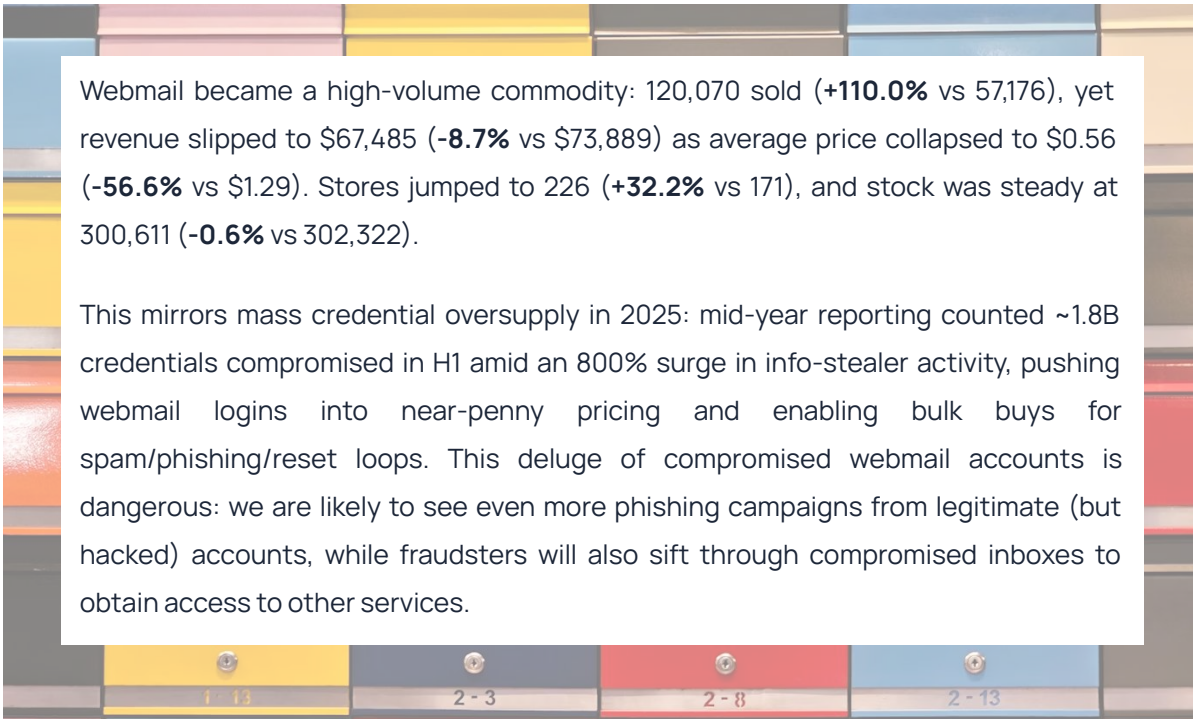
96% ▲
Account Sales

4% ▲
Revenue

1% ▼
Active Shops

6% ▲
Total Stock

WEBMAIL



Webmail became a high-volume commodity: 120,070 sold (**+110.0%** vs 57,176), yet revenue slipped to $67,485 (**-8.7%** vs $73,889) as average price collapsed to $0.56 (**-56.6%** vs $1.29). Stores jumped to 226 (**+32.2%** vs 171), and stock was steady at 300,611 (**-0.6%** vs 302,322).

This mirrors mass credential oversupply in 2025: mid-year reporting counted ~1.8B credentials compromised in H1 amid an 800% surge in info-stealer activity, pushing webmail logins into near-penny pricing and enabling bulk buys for spam/phishing/reset loops. This deluge of compromised webmail accounts is dangerous: we are likely to see even more phishing campaigns from legitimate (but hacked) accounts, while fraudsters will also sift through compromised inboxes to obtain access to other services.

110% ▲
Account Sales

9% ▼
Revenue

32% ▲
Active Shops

1% ▼
Total Stock

GUN-RELATED AND WHITEPAGES PREMIUM ACCOUNTS FOR SALE

This quarter, Kasada IQ observed an anomaly in ATO activity that raised significant concerns. Kasada IQ identified three criminal marketplaces selling accounts for US-based online gun dealers. These same three marketplaces are also selling accounts for WhitePages Premium accounts. One of the marketplaces (“Marketplace A”) stocks the majority of accounts, holding **93%** of stock for the gun-related accounts and **94%** of the WhitePages accounts.

This demonstrates a change in the market. Kasada IQ does not often see these kinds of accounts targeted for credential stuffing and ATO, noting there are more restrictions and legislation that apply. Kasada notified the relevant companies in August 2025.

GUN-RELATED ACCOUNTS

The accounts listed were for a self-described online gun dealer based in the US. The retailer sells firearm and shooting-related equipment, including ammunition, accessories, parts and gear. Priced at USD $4 to $8, the accounts are easily accessible.

155	155
Total Accounts Sold	Total Stock

Adversaries frequently sell and use stolen accounts with payment methods attached. In this case, the three marketplaces expressly sell accounts to be used to purchase items. Each marketplace provides instructions on how to successfully use the account to check out items from the website.

There are mechanisms in place to prevent illegal purchasing of firearms and, to a lesser extent, ammunition. However, the retailer sells other items, including firearm parts, consumer optics, tools and tactical wear. Ammunition is an expensive and in-demand product, making it an attractive target for fraud and reselling in criminal networks. Outside of potential criminal offences, using the stolen accounts positions buyers to get caught out by online firearms purchase requirements.

WHITEPAGES ACCOUNTS

WhitePages accounts are marginally more common than gun-related accounts on criminal marketplaces. Kasada IQ has observed at least 8 criminal marketplaces selling accounts for WhitePages. What is more concerning is the three marketplaces selling gun-related accounts and WhitePages Premium accounts in the same place. Priced at USD $1.5 to $15, these accounts are also easily accessible.

150	7,180
Total Accounts Sold	Total Stock

Notably, Marketplace A, which Kasada IQ has previously looked into for unethical activity, offers WhitePages Premium accounts with Background Reports enabled. Background Reports present in-depth, sensitive data about an individual which could be used to dox, intimidate, coerce, stalk or otherwise harass selected individuals. Data contained in Background Reports can also help bypass predetermined security questions from institutions.

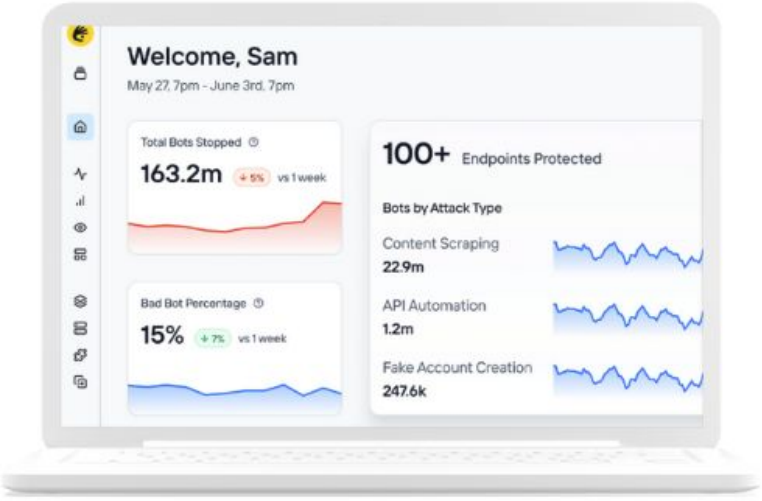
Looking Ahead

Threat Intelligence at Kasada

Kasada uses threat intelligence to drive the identification of new and emerging threats, techniques and tactics used by adversaries. This identification, coupled with broad access and analysis of open and closed data sources, allows Kasada to rapidly implement new mitigations or identify alternate methods to reduce the impact of automated threats, bot attacks, and online fraud.

The people we're up against are dynamic, well-resourced, and technically proficient. This evolving field means that Kasada needs to be at the forefront of cybersecurity to provide subject matter expertise relating to the capabilities, development pipeline, and targets of specific actors or groups against their networks.

The goal of threat intelligence within Kasada is to reduce the efficacy of the threat ecosystem by providing complete, accurate, relevant, and timely intelligence to customers.



How Kasada IQ can help

- **Unparalleled insights into the adversary ecosystem**. Our collection consists of deep access across 2000+ unique collection locations, with over 23 million messages ingested each month.
- **Deep expertise on the automated threat landscape, adversary behavior and intelligence practice.** Dedicated analyst hours can help you dig deeper to investigate what's most relevant to your needs – whether that's intelligence on fraud groups, reverse-engineering, or pinpointing security weaknesses in your environment.
- **Adversary engagement.** We bridge the gap between you and the adversary to help better understand behaviors and patterns.
- **Threat reporting.** We equip you with regular cadence reporting on relevant trends at the organization and/or industry level, tailored for all levels of audiences across your organization.

https://www.kasada.io/

enquiries@kasada.io

team-threat-intel@kasada.io

Connect with kasadaiq on: