kasada

Quarterly Threat Report

Q1 2025

Table of Contents

Introduction

Welcome to Kasada's Q1 2025 Quarterly Threat Report, where we arm 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 KasadaIQ in Q1, this report cuts through the noise and pulls out the key areas your organisation needs to focus on to stay ahead of the curve. All insights are based on analysis and investigations via our in-house KasadaIQ intelligence capability, supported by deep access to open and closed sources and decades of technical and intelligence expertise combined.

Intelligence requirements

This report provides insights against the following intelligence requirements:

- What were the top automated threats observed by KasadaIQ in Q1 2025?
- How did the top automated threat observed by KasadaIQ in Q1 2025 impact key industries?
- What movements in the automated threat landscape did KasadaIQ observe in Q1 2025?
- Which automated threat required the most attention in Q1 2025?

How to read this report

- Threat Landscape Update - Provides an overview of the top threats tracked by KasadaIQ over the past quarter, key industry trends and notable events across the landscape.
- Spotlight on: ATO and its enablers - Provides a deep dive into Kasada's focus area for the past quarter, which for Q1 was ATO, using a "what", "who", "why" and "how" model. Includes:
    - Adversary Insights
    - ATO metrics in Q1
- How we can help - Provides an overview of how KasadaIQ can empower you with intelligence and the kinds of questions we can help you answer to meet the threats discussed in this report.

Threat Landscape Update

ATO remained the **most frequent and impactful threat**.

Stolen accounts **far exceeded** other listing types on criminal marketplaces, including gift cards and configurations.

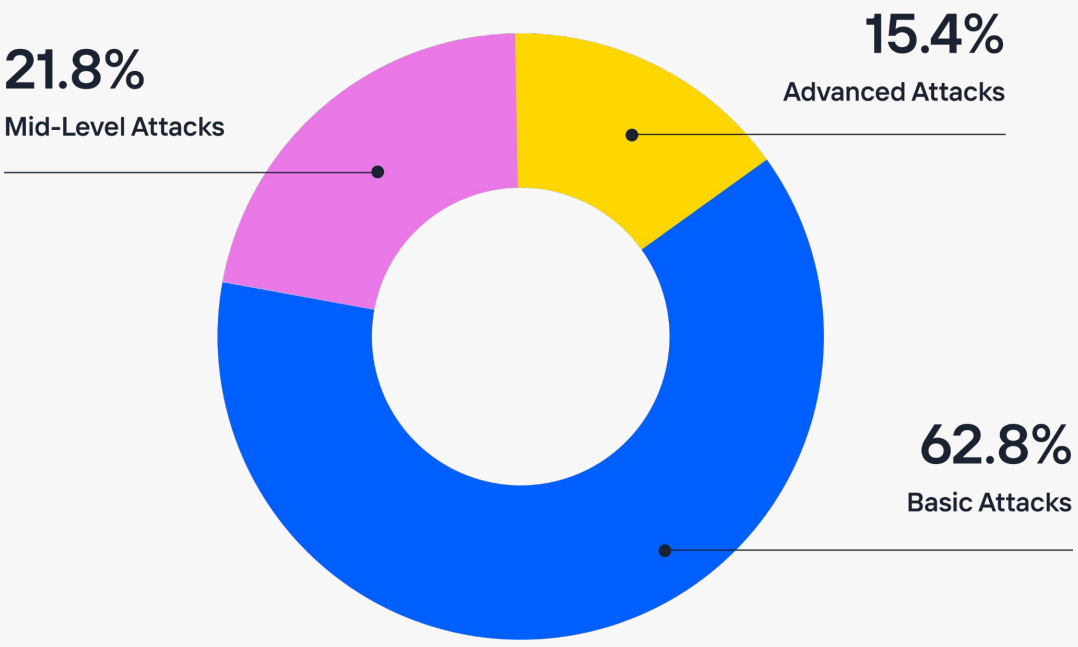
Criminals are diversifying ATO operations to include **welfare** and other kinds of benefits.

OpenBullet configuration developers are abusing **CAPTCHA solver services** without KYC requirements.

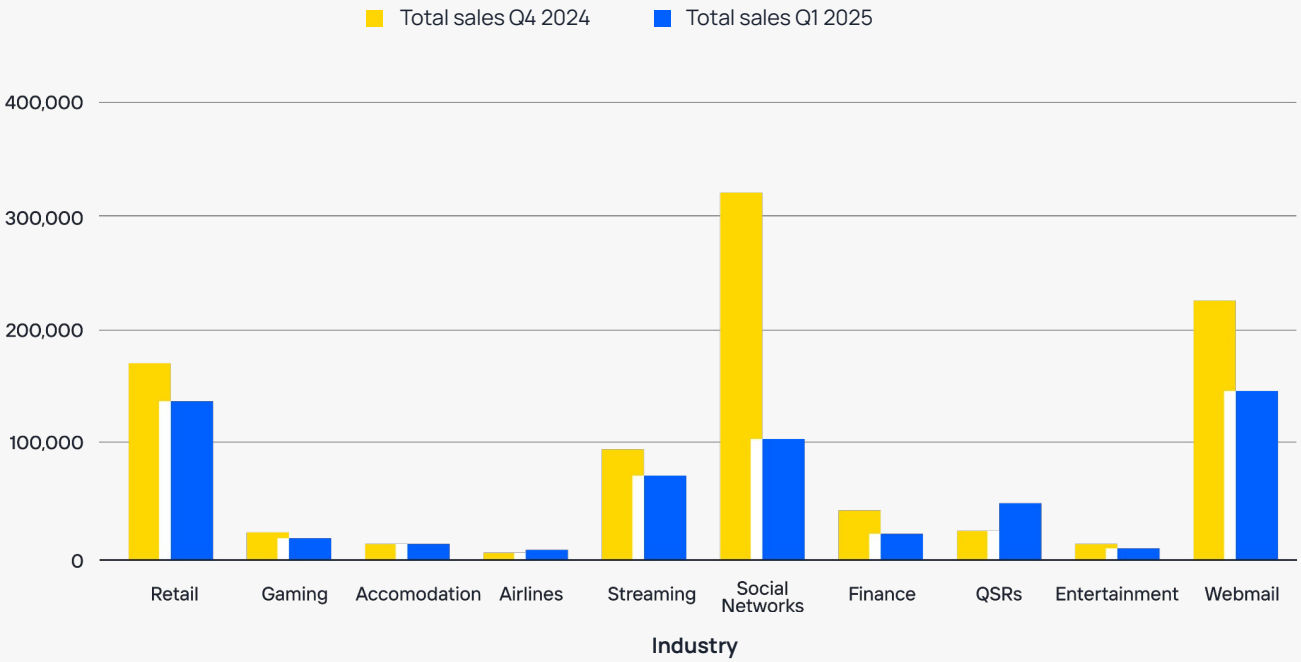
Retail and hospitality related industries remain **top targets** for automated threats.

Adversaries and industry are increasingly focused on **scraping**.

Sophistication of bot activity observed by Kasada varied, with the majority of attacks assessed as basic. In Q1, the majority of bot activity observed demonstrated little evasion capabilities and obvious signs of automation.



The top three most targeted industries for ATO and credential stuffing were webmail services, retail and social networks. Collectively, these industries constituted **67%** of all account sales tracked by KasadaIQ in Q1 2025.



See Spotlight on: ATO and its enablers.

Analyst Insights

Based on observations from our KasadaIQ analysts in Q1 2025, below are some key insights to keep in mind for Q2 2025.

- In Q1 2025, we observed a resurgence of reselling communities and a renewed focus on hype goods. While there are less active bots and bot users than this time last year, those that have survived are gaining momentum.
- With several special events, holiday periods and scheduled hype item drops in Q2 2025, there will be several opportunities for reselling communities to put this renewed focus to use.

We expect to see further resurgence of reselling communities and refocusing on hype items.

[1] https://www.conference-board.org/topics/consumer-confidence

- In Q1 2025, US consumer confidence continued to drop, with near-term outlook for incomes, business and labour market conditions falling to the lowest in 12 years and below the threshold that usually indicates an impending recession.
- Towards the end of Q1 2025, uncertainty around the impact of the US President's economic measures, including import tariffs, peaked.
- These developments may have flow on impacts for pricing decisions and models for businesses in the United States and globally.
- Criminals are known to exploit features of uncertain economic conditions, including reduced security budgets in businesses facing financial strain and consumer stress.
- Against this backdrop, criminals, like ALTSRUS, are stealing accounts connected to welfare benefits cards. See ALTSRUS - THE REVERSE ROBIN HOOD.

Uncertain macroeconomic conditions may increase the risk appetite of adversaries, the vulnerability of consumers and increase competition over Q2 2025.

- The sale of stolen accounts during Q1 2025 was heavily impacted by the 29 January seizure of `Sellix.io` by law enforcement as part of Operation Talent.
- Sellix was a digital marketplace platform and payment processor that enabled its users to build shopfronts and sell digital goods. At the time it was seized by law enforcement, Sellix accounted for 43% of all criminal marketplace shopfronts monitored by KasadaIQ.
- In an over decades long pattern of behaviour, adversaries have rapidly shifted to fail gaps in their operations, largely due to the dynamic and organised nature of criminal supply chains (see ALTSRUS - THE REVERSE ROBIN HOOD).
- KasadaIQ observed several operators quickly adopting new shops to replace Sellix within 24 hours of it being seized.

We expect the impacts of law enforcement takedowns of criminal marketplaces and infrastructure to remain temporary in Q2 2025.

- In Q1 2025, several new and improved AI models and agents were released with enhanced functionality.
- Already in 2025, we have seen at least 12 mainstream releases of new generative AI functionality, expanding to hybrid reasoning and hyper-realistic image generation.
- In parallel, KasadaIQ continues to observe ways in which adversaries could use this technology to benefit their operations. This includes generating fake receipts, automating returns and placing recurring orders.

Adversaries continue to exploit emergent AI agents and capabilities to increase the scale and efficiency of their operations, despite developer safeguards.

- KasadaIQ expects to see an increased focus on web scraping throughout 2025, driven largely by the need for multi-media data acquisition to inform AI and machine learning. As multi-modal AI continues to grow, market demand for scraping will likely expand to image, audio and video.
- For the last 12 months, KasadaIQ have monitored the emergence of no and low code scraping capabilities, which reduce the barriers to entry for lower skilled operators.
- In some instances, our custom defences have forced adversaries to invest more resources in bypassing protections. This included a commercial scraper increasing the pricing for all domains protected by Kasada.
- Identifying and addressing unauthorised scraping is complex. While some anti-bot solutions focus purely on feeding adversaries realistic but irrelevant content, KasadaIQ notes the importance of a tailored, multi-level approach to increase the costs for developers and decrease the threat sustainably over time.

Both adversary and industry attention towards scraping is increasing, and for good reason. Custom defenses are critical in increasing the costs for adversaries.

Spotlight on: ATO and its Enablers

In February 2025, Kasada released its **Account Takeover Attack Trends 2025**, reporting that ATO incidents surged by **250%** with over **6.8 million** accounts listed for sale on criminal marketplaces in 2024. In Q1 2025, KasadaIQ availability of stolen accounts far exceeded other listing types observed by KasadaIQ on criminal marketplaces. Stock of stolen accounts on criminal marketplaces peaked in early January, with nearly **2.5 million** available for sale. This is approximately 37% of all account listings observed in 2024.

KasadaIQ assesses the overall threat of ATO to be **HIGH**.[2] The speed and scale at which adversaries are conducting and evolving ATO attacks highlights the criticality of proactive threat intelligence in increasing the costs for adversaries and decreasing the risks for potential targets.

ATO can have significant consequences for individuals and businesses. Business impacts can include reputational damage, loss of consumer trust, financial losses, negative customer experience and regulatory action. Personal impacts can include financial losses, breaches of sensitive data or other private information and inability to access accounts.

Profiling ATO

WHAT

ATO is a type of fraud where adversaries gain access to your accounts and critical data. The primary targets of ATO include:

- User accounts.
- Authentication systems.
- Password reset flows.
- Loyalty programs.

See ATO metrics in Q1.

WHY

The primary objectives of ATO include:

- Unauthorised access to accounts.
- Credential marketplace sales.
- Fraud monetisation.
- Access to stored value (points, credit).

[2] This is based on an assessment of aggregate intelligence holdings and is not nuanced by industry breakdown. This threat rating is based on analysis of capability, impact and, to a lesser extent, intent.

WHO

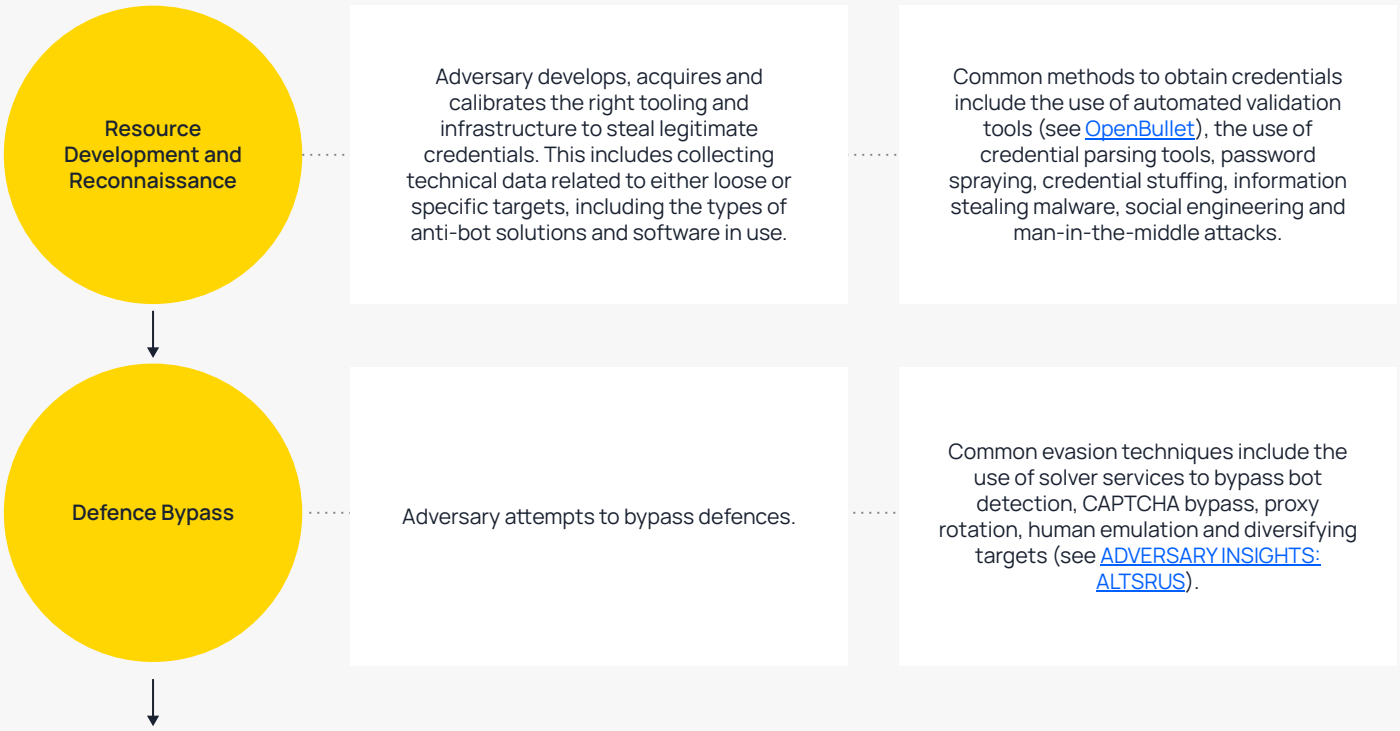
ATO is generally conducted by cyber criminals and fraud and abuse syndicates. Cybercriminals and active facilitators of fraud are opportunistic, organised and highly adaptive. There are several operators across the criminal supply chain that facilitate end-to-end fraud operations, including criminal marketplaces. See ALTSRUS - THE REVERSE ROBIN HOOD.

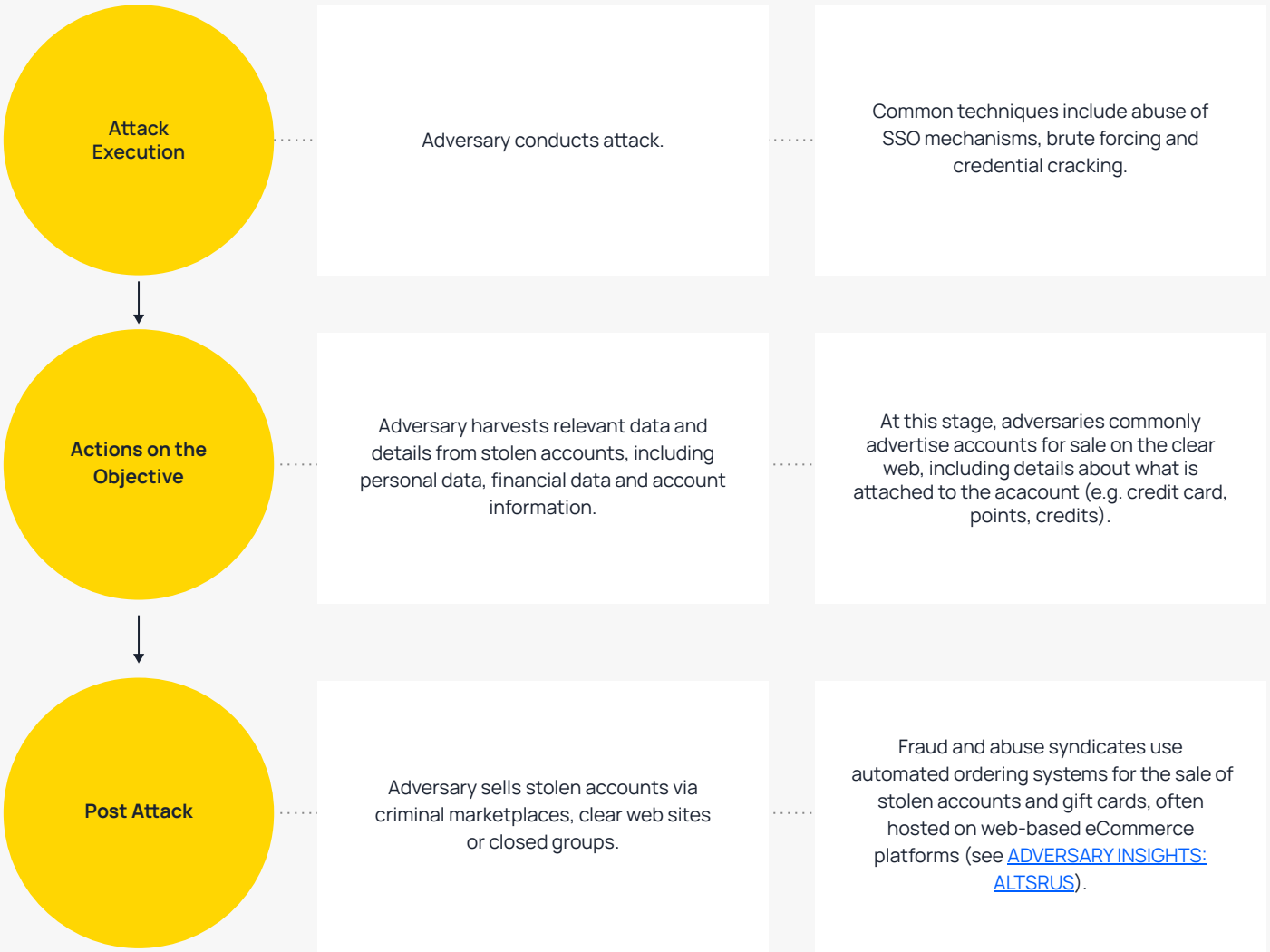
Overall, we assess adversaries behind ATO have a high capability level based on the considerations below.

Technical capability	Access to resources	Scale	Persistence
High	Moderate-High	Moderate	High

HOW

Adversaries take over accounts by stealing the victim's login credentials, using malware, or finding and exploiting vulnerabilities in the security of the accounts.





See OPENBULLET AND THE CAPTCHA WITHIN.

Adversary Insights

ALTSRUS - THE REVERSE ROBIN HOOD

KasadaIQ generally observes fraud groups targeting consumers of large retailers and corporations. However, we recently observed a prolific fraud group, ALTSRUS, stealing accounts connected to Electronic Benefit Transfer (EBT) cards and pharmacy scripts. By going after accounts with EBT cards attached, ALTRUS is going that one step further by targeting those in society already facing challenges and disadvantages. To be eligible for an EBT card, a household must have a monthly income that falls below the poverty line. For a household of one individual, their net income for Q1 2025 would have to be below $3,765 USD to be eligible for EBT.[3] In the same period, ALTSRUS' revenue generated totaled $589,729 USD, approximately **157 times** the income of EBT card holders in the United States.

EBT is an electronic system in the United States that allows a participant of the Supplemental Nutrition Assistance Program (SNAP) to pay for food using SNAP benefits.

SHOOTING LOW BUT WIDE

ALTSRUS currently sells stolen accounts, promotional codes and gift cards for organisations primarily in the United States.[4] ALTSRUS employs a range of techniques to gain access to accounts and gift cards, including using automation to brute force account credentials and gift card numbers, as well as searching breached email accounts for potential credentials and gift card identifiers.

SOME NOT SO MERRY FIGURES

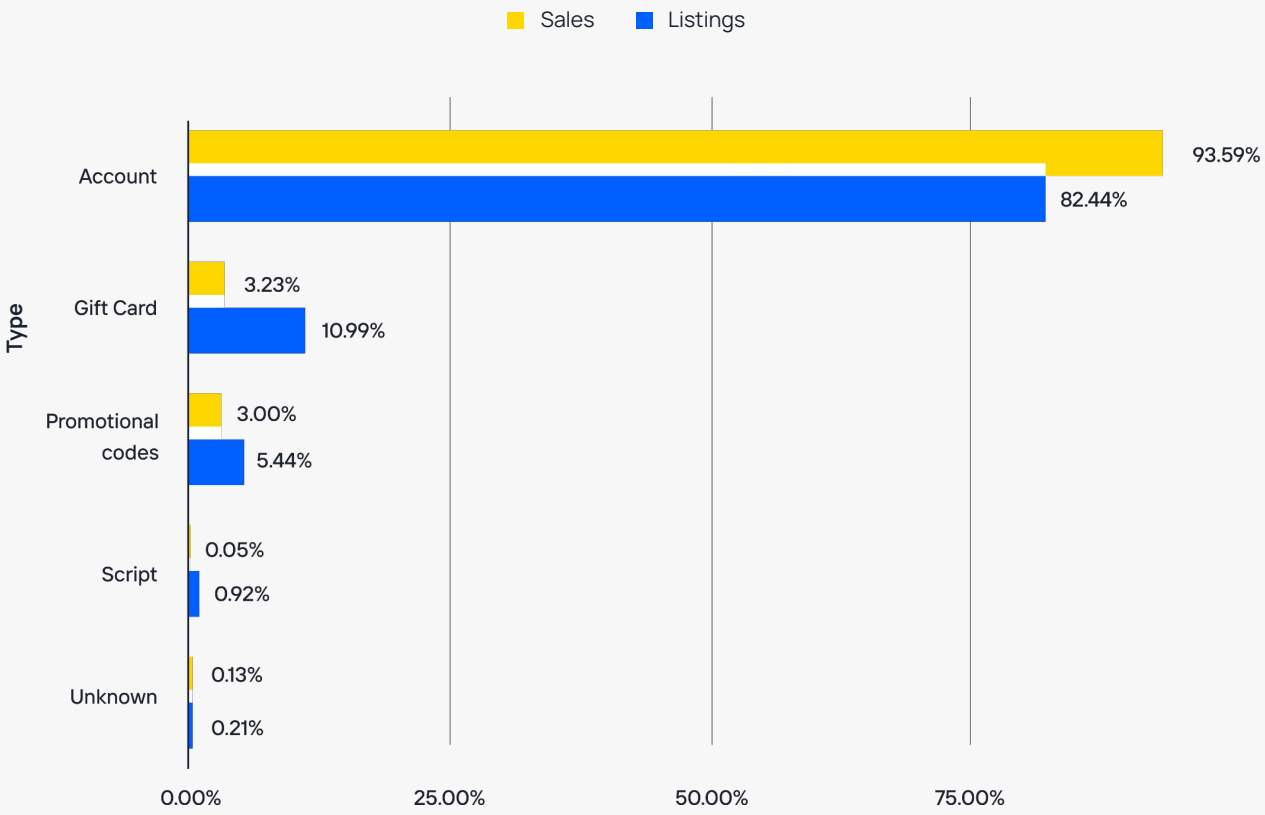
KasadaIQ has observed ALTSRUS activity on criminal marketplaces as early as April 2020. Since December 2022, ALTSRUS has gradually increased year-on-year, with spikes in activity observed in the June-July period. In Q1 2025, KasadaIQ observed a significant scaling and diversification of ALTSRUS' operation compared to Q1 2024.

Unique listings in Q1 2025 increased to 974, about a **2,852%** increase when compared to Q1 2024.

[3] http://fns.usda.gov/snap/recipient/eligibility

[4] There are limited prior listings in Canada and Europe.

In Q1 2025, ALTSRUS' listing types **more than doubled** compared to Q1 2024, expanding to include gift cards, promo codes and pharmacy scripts.

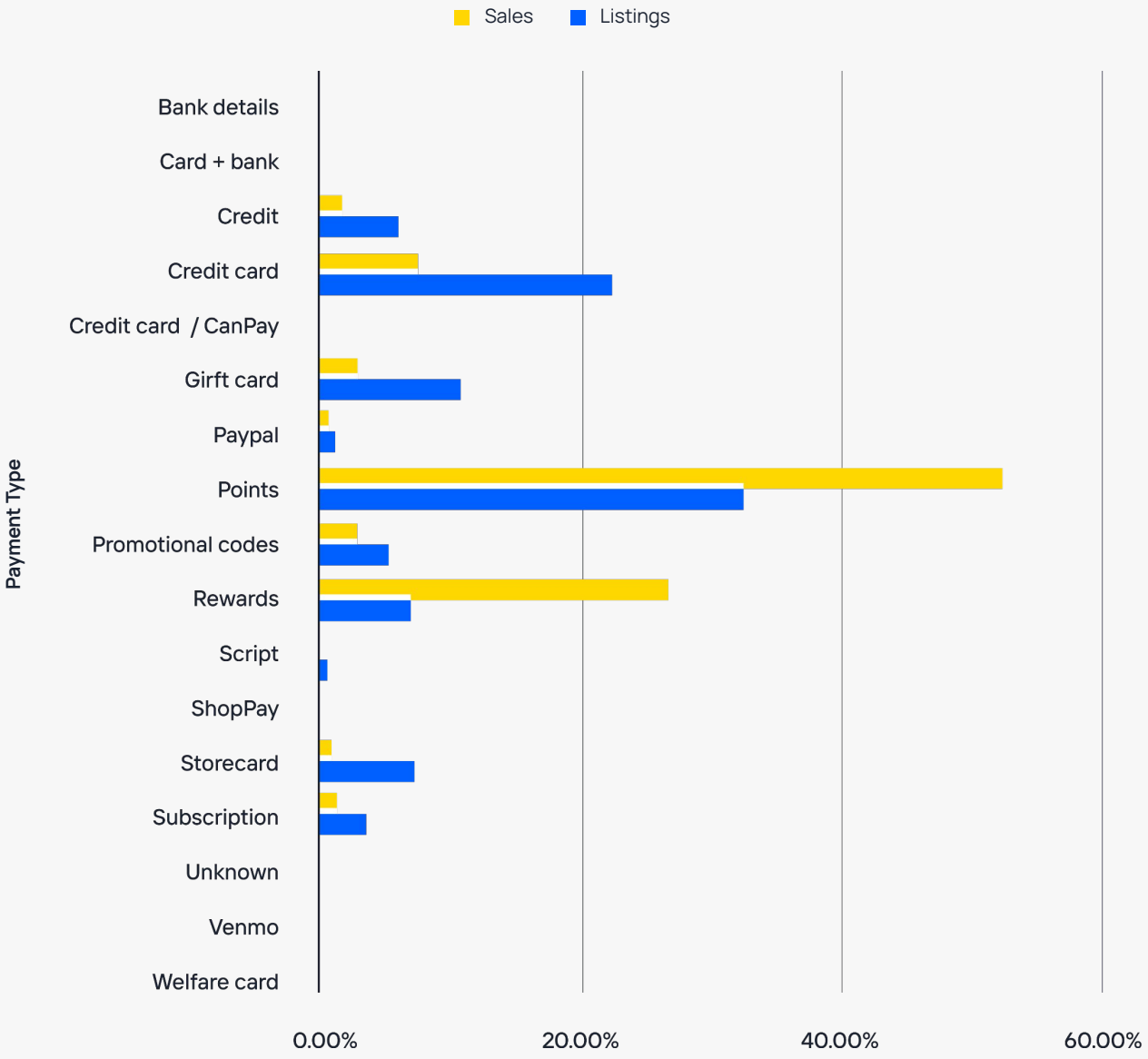


- ALTSRUS lists consumer accounts with a United States pharmacy chain with **17** different types of prescriptions ready to refill. Many of the prescriptions are for severe pain management, mental health issues and quality of life - preventing individuals in society from accessing their prescribed medication when they really need it.
- In Q1 2025, **accounts** constituted the majority of listings and sales on ALTSRUS, followed by gift cards and promotional codes.

Sales increased to 220,240, an approximate **570%** increase when compared to Q1 2024.

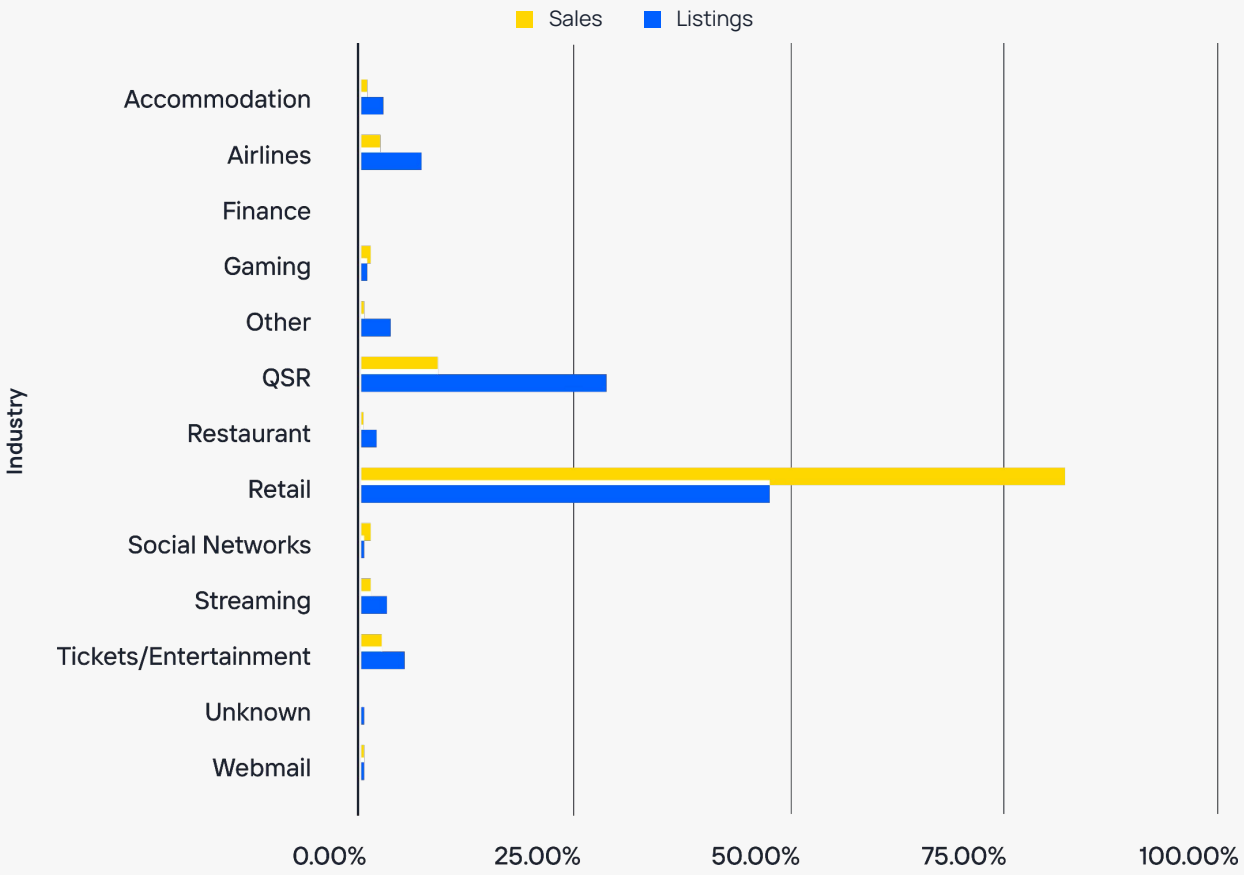
Total revenue increased to $589,729 USD, an approximate **734%** increase compared to Q1 2024.

In Q1 2025, attachments to accounts listed on ALTSRUS, like points and credit cards, increased **143%** when compared to Q1 2024. This included listing accounts linked to EBT cards.



- In Q1 2025, **points** were the most common attachment to accounts sold, followed by rewards and credit cards.

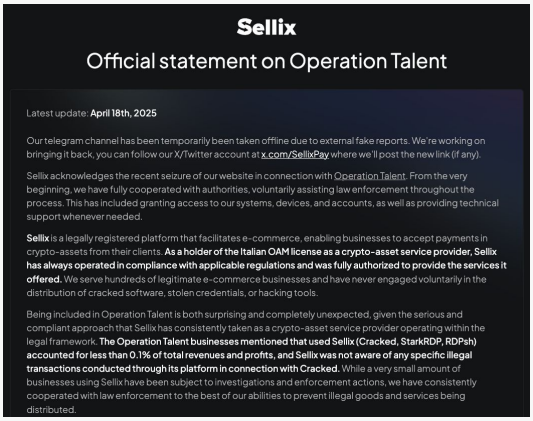
The number of industries targeted by ALTSRUS increased by **85%** when compared to Q1 2024.



- In Q1 2025, **retail and hospitality** related industries, led by retail and QSRs, constituted approximately **85%** of all listings and **94%** of all sales observed by KasadaIQ.
- Retail and hospitality related industries are highly attractive targets for ATO due to the high volume of account activity, diverse payment methods attached to accounts and ease of access.
- Adversaries invest significant resources into targeting eCommerce platforms to steal data at scale.

CRIMINAL PLATFORMS RISE AND RISE AGAIN

It is plausible that the significant spike in ALTSRUS listings from February 2025 was influenced by the 29 January law enforcement seizure of web-based eCommerce platform, Sellix. This platform was used by criminals to facilitate illicit sales of stolen account information.



Cybercriminals and facilitators are opportunistic, organised and highly adaptive, rapidly shifting to fill gaps in their operations - when one cog in the criminal supply chain disappears, another surfaces to take its place. This pattern of behaviour has been observed for over a decade, looking back to the re-emergence of online black market, Silk Road 2.0, only a month after the initial, first-of-its-kind Silk Road website was shut down by the FBI.

More recently, we watched this play out with the emergence of BreachForums in response to the 2022 law enforcement takedown of criminal marketplace, RaidForums. When RaidForums was disrupted, a prolific user spun out BreachForums to continue its legacy. Similarly, BreachForums continues to operate today despite a disruption in 2023, when a user and former administrator reopened the forum. When these new platforms surface, KasadaIQ often observe increased investment in operational security. For instance, KasadaIQ has observed some fraud adversaries migrating their business to Discord and Telegram to emulate shop fronts. This allows the administrators of these servers and channels to restrict access, decreasing their risk of being shut down.

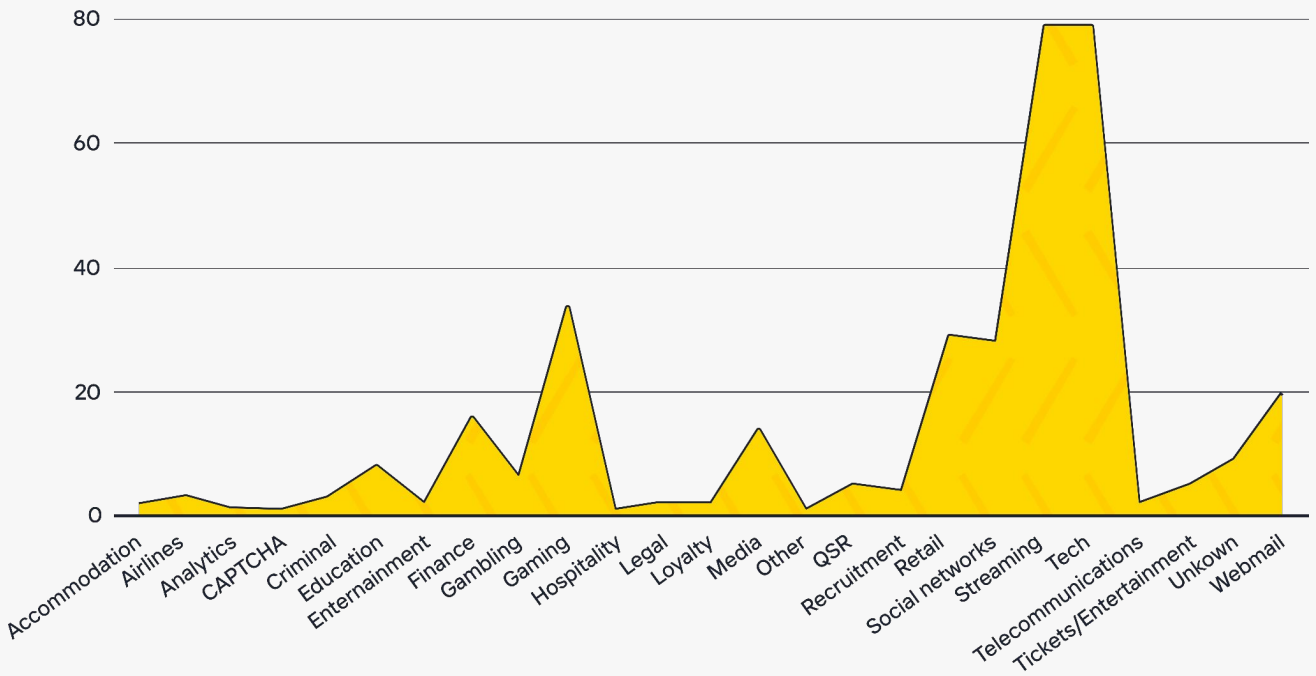
KEY CONSIDERATIONS FOR BUSINESSES

- **Do you have adequate visibility of criminal marketplaces, external breaches and adversary activity to understand your exposure?** A key challenge for businesses is that these accounts are often stolen from third party providers, like webmail services, and are outside of their remit of monitoring and control.
- **Do you have measures in place to detect and prevent early indicators of ATO, like increased login failures, unusual geographic access and spikes in login attempts?** Addressing credential stuffing early in the attack chain is critical in safeguarding customer accounts.
- **How do you support consumers in preventing their accounts being taken over?** ATO and credential stuffing relies on password reuse. Password and security policies for accounts registered with your business should prescribe good baseline security.

OPENBULLET AND THE CAPTCHA WITHIN

OpenBullet is a legitimate open source penetration testing tool abused by adversaries to perform credential stuffing and ATO attacks against publicly accessible websites. Website-specific configuration files ("configs") that are shared within criminal communities enable unsophisticated adversaries to automate credential stuffing attacks against the specified website.

In Q1 2025, KasadaIQ observed **361** OpenBullet configs listed by adversaries. The top industries for configurations observed were streaming (**~22%**), technology (**~22%**), gaming (**~10%**), retail (**~8%**) and social networks (**~8%**).



CAPTCHA SOLVING PROVIDERS PASSIVELY FACILITATING FRAUD

OpenBullet integrates with CAPTCHA solvers, meaning adversaries can bypass CAPTCHA systems that are designed to stop automated attacks or use CAPTCHA solvers to register new accounts on websites which can be used in criminal activities. Kasada has previously reported on CapSolver, a China-based solver service which is known to actively advertise its services on deep web criminal and hacking forums.[5]

However, in Q1 2025, KasadaIQ observed several configs developers relying on CAPTCHA solving providers which operate as legitimate businesses and do not demonstrate intent to engage or support malicious activity. Instead of actively facilitating criminal activities, CAPTCHA solver services without know your customer (KYC) requirements in place are being abused to passively facilitate criminal activities.

Below are examples of two of the different types of CAPTCHA solving services we identified.

Human-powered	AI-powered
• Malicious intent not identified.	• Malicious intent not identified.
• Legitimate business presence on self-run website and LinkedIn.	• Legitimate business presence on self-run website and LinkedIn.
• Offers solvers for 27 different types of CAPTCHAs.	• Supports reCAPTCHA, Solve Media and over 27,500 image captchas.
• Pay per 1000 solves.	• Operates through a subscription model.
• Solving time of between 3 and 50 seconds.	• Offers unlimited solves.
• Relies on a workforce of individuals who manually solves the CAPTCHA and sends answers to their service.	• Relies on AI to solve CAPTCHAs.
• Has Terms of Service stipulating that the service must only be used for authorized and legal purposes, in accordance with applicable laws and regulations.	• Has Terms of Service stipulating that the service must only be used for authorized and legal purposes, in accordance with applicable laws and regulations.

CAPTCHA LATER - TIME TO DITCH THE CAPTCHA

Kasada's view is that CAPTCHAs are largely ineffective and continue to be outsmarted by adversaries, AI and bots, while frustrating customer experience. Anti-bot solutions using CAPTCHA challenges are more vulnerable to solver services and a broader range of threats.

Not only are CAPTCHAs ineffective in preventing fake telemetry getting through and stopping their puzzles being automated, they are actually helping adversaries improve the believability and pervasiveness of their information stealing efforts, which ultimately drive other automated threats (like ATO) to businesses and consumers. As multi-modal AI is increasing the scale and effectiveness of CAPTCHA solving[6], and criminals weaponising CAPTCHAs in malicious social engineering and malware deployment campaigns[7], it is well and truly time to ditch the CAPTCHA.

[5] https://www.kasada.io/q4-2023-threat-report/

KEY CONSIDERATIONS FOR BUSINESSES

- **Are CAPTCHAs impacting your customer experience and bottom line?** CAPTCHAs frustrate real users and discourage conversions. With cart abandonment rates sitting at around 70% for online retail orders, emphasis on seamless and positive customer experience is paramount.[8]
- **Do you have visibility of criminal marketplaces and listings relevant to your business or industry?** You cannot protect what you don't know about. Configs are relatively easy to launch and can have devastating consequences, such as data breaches and loss of customer trust.

[6] https://www.kasada.io/captchas-demise-multi-modal-ai/
[7] https://www.kasada.io/fake-captcha-scams-ruining-consumer-trust-and-driving-website-abandonment/
[8] https://baymard.com/lists/cart-abandonment-rate

ATO Metrics in Q1 2025

In Q1 2025, the availability of stolen accounts far exceeded other listing types, like gift cards and OpenBullet configs. Stock of stolen accounts peaked in early January, with nearly **2.5 million** available for sale. Law enforcement action against the Sellix.io platform on 30 January resulted in a 50% reduction of observed stock numbers. KasadaIQ introduced expanded monitoring on 18 February, enhancing visibility into criminal marketplaces. An outage between 21 and 24 February briefly reduced this visibility, before ongoing monitoring was restored.

ACCOUNT SALES BY INDUSTRY

- The impact of the seizure of Sellix.io on 30 January by law enforcement was not equal across all industries;
  - Stock of social network accounts was particularly impacted, dropping 95%.
  - Entertainment, retail and quick service restaurants saw negligible decline.
- Kasada expanded monitoring on 18 February, enhancing visibility into criminal marketplaces. As a result, observed stock of retail accounts increased 188%.

	Total Sales	Stores Selling Accounts	Maximum Available Stock	Average Account Price
Accommodation	13,403↓	29↓	80,684↑	$4.15↓
Airlines	9,207↑	45↓	86,774↑	$29.79↓
Entertainment & Ticketing	10,851↓	64↓	109,913↑	$7.43↑
Gaming	19,139↓	280↓	242,317↓	$0.91↓
Quick Service Restaurants	48,321↑	120↓	367,238↑	$3.06↓
Retail	138,032↓	360↓	921,085↑	$2.47↓
Social Networks	104,166↓	331↓	677,266↓	$0.45↑
Streaming	72,840↓	565↓	370,886↓	$2.57↓
Webmail	147,028↓	130↓	220,027↓	$0.38↑

ACCOMMODATION

Kasada observed approximately 13,400 accommodation and hotel/motel account sales in Q1 2025. This represented a 9% decrease when compared to Q4 2024. The slight decline in volume can likely be explained by seasonal fluctuations in demand following the December/January holiday period.

The average sale price of stolen accounts reduced slightly, from $4.75 to $4.15 USD. Accounts for hotel chains are typically valued higher than many other types of accounts due to the redeemable rewards points that are included; these often have a specific dollar value attached. The high value of hotel accounts was offset by the relatively low value of homestay service (i.e. Airbnb, etc) accounts, which sold for as little as $0.50 USD per account.

AIRLINES

Observed sales of stolen airline accounts increased quarter-on-quarter by over 33%, up to approximately 9,200. This increase was driven mostly by Kasada's enhanced visibility into criminal marketplaces, and due to the fact that few sellers of airline accounts relied on Sellix as a platform.

Airlines were second only to retail as the most lucrative industry to target by ATO specialists. Frequent flyer and air mile programs remain high value targets for criminals looking to cash out, and the average price of nearly $30 USD per account reflects this high value.

Available airline account stock similarly increased approximately 50% to peak at nearly 87,000 in Q1. As per the sales numbers, this increase can be attributed to an expansion of Kasada's monitoring capabilities.

▲ 33%

Stolen airline customer accounts increased **33%** from Q4 2024 to Q1 2025.

ENTERTAINMENT & TICKETING

Event ticketing services remain a high value target for ATO specialists. Using automated open source tools like OpenBullet, an attacker can perform a credential stuffing attack and automatically categorise compromised accounts by which tickets have been purchased. Customers who purchase these accounts can then transfer the tickets to their own account, or attempt to attend the event before the legitimate ticket holder. Victims of these attacks are often left without adequate compensation.

Sales of event ticketing accounts dropped by approximately 28% quarter-on-quarter, with numbers down to just under 11,000. The Sellix.io seizure had a negligible effect on the sale numbers of accounts, with the reduced numbers coming from lower total demand.

At the same time, the average price of a sold account increased by 87% to $7.43 USD, with overall revenue increasing by 31%. This indicates that the demand for high value tickets – such as sold out music tours – has increased, while demand for lower value tickets – cinema passes – has decreased.

GAMING

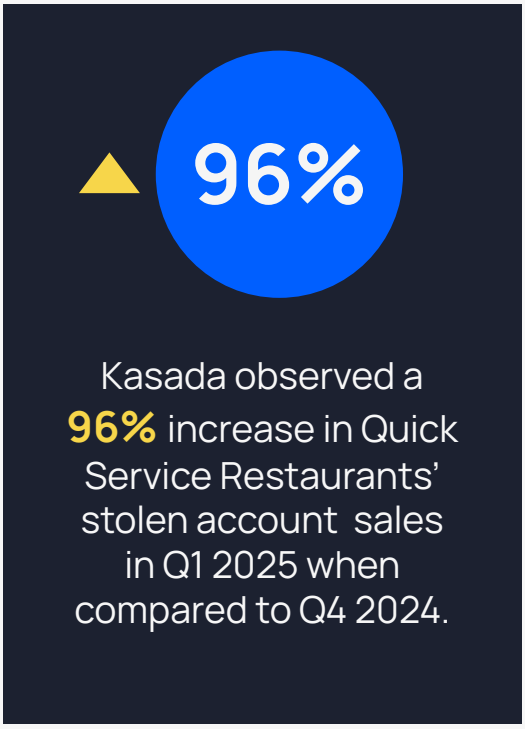
Demand for stolen gaming customer accounts was consistent across Q1 2025, with no major high profile releases during the quarter. Total sales declined approximately 22%, from 24,500 to 19,000, which can mostly be attributed to the lack of high profile game releases.

Stock of available gaming accounts was heavily impacted by the seizure of Sellix.io. Stock numbers dropped by 41% after the law enforcement action, down to 144,000 from a peak of 242,000. While some shops migrated to other platforms, many sellers had not moved by the end of the quarter.

QUICK SERVICE RESTAURANTS (QSR)

Demand for Quick Service Restaurants (QSR) compromised accounts rapidly increased in Q1. Kasada observed a 96% increase in sales when compared to Q4 2024, up to 48,000. While some of this increase can be attributed to expanded criminal marketplace monitoring, we have also seen increased activity within criminal communities targeting quick service restaurants.

As more restaurants offer various forms of loyalty programs, their customer accounts become more lucrative to criminals performing ATO attacks. Using open source automated tools like OpenBullet, these attackers are able to quickly compromise dozens of accounts and ascertain how many loyalty points are available to each account.



Customers then purchase these accounts, at an average price of just over $3.00 USD, log in, and buy a meal using loyalty points. This type of fraud is seen as relatively low risk among the community, with users often posting testimonials about successfully redeeming loyalty points for meals. The seizure of Sellix.io had a negligible effect on the sale or stock numbers of stolen QSR accounts.

RETAIL

Observed sales of stolen retail accounts dropped approximately 19% from Q4 2024 to Q1 2025, down to 138,000. Demand peaked at the start of the quarter, as purchasers looked to take advantage of post-holiday sales.

Stock numbers of retail accounts were not noticeably affected by the seizure of Sellix.io. Kasada's increased monitoring footprint, implemented on 18 February, impacted retail account stock levels more than any other industry; observed stock levels increased 188% to 921,000.

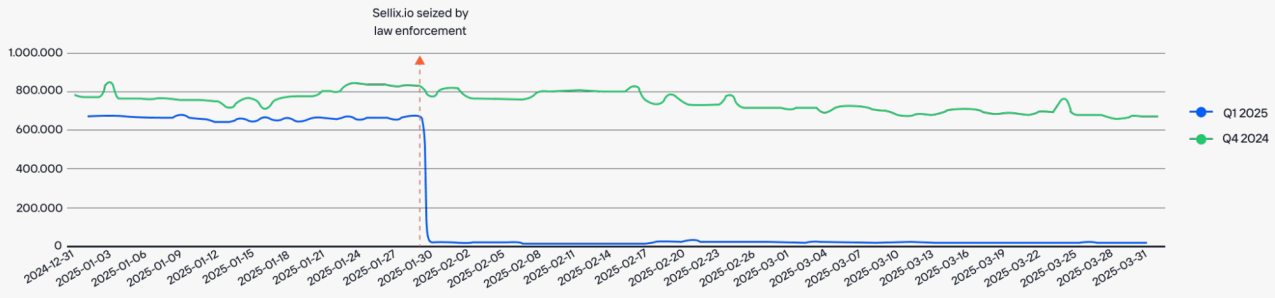
Kasada increased its monitoring footprint, and retail stolen account stock levels rose **188%**, in Q1, more than any other industry.

▲188%

SOCIAL NETWORKS

The sale of stolen social networking accounts was the hardest hit by the seizure of Sellix.io, with sales dropping 67% when compared to Q4 2024. The average sold price of a social network account remained low, at under $0.50 USD.

The impact of the Sellix.io shutdown was even more dramatic when looking at the available stock of social network accounts. Prior to January 30, approximately 670,000 stolen accounts were available for sale. Following the seizure, that number dropped by over 95%, to just over 19,000.



STREAMING

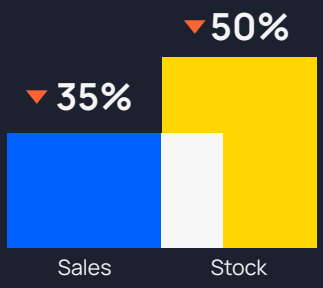
Observed sales of stolen streaming accounts dropped approximately 21% between Q4 2024 and Q1 2025, to almost 73,000. It is likely that much of this drop can be attributed to the Sellix.io seizure, as available stock levels saw a 57% reduction following the law enforcement action.

As streaming services continue to increase in price and further fragment, the discussion around stolen streaming accounts within criminal communities has increased. Using these accounts is seen as low-risk within the community, and sellers often provide detailed instructions on how to reduce the chance that a legitimate account owner will notice that they've been compromised. Some sellers advertise a 'lifetime warranty' on streaming accounts, reflecting confidence in their supply pipeline.

WEBMAIL

Webmail accounts are generally sold in bulk, and are often used as a first step towards compromising other, more lucrative accounts. Criminals will use automated tools to search through hundreds or thousands of compromised webmail inboxes for credentials or login information for other services.

Compromised webmail accounts remained cheap in Q1 2025 at $0.38 USD, but both sales and available stock were also impacted heavily by the seizure of Sellix.io. Sales dropped nearly 35% to 147,000, and stock was down almost 50% to 130,000 by the end of the quarter.



Sales of webmail accounts dropped nearly **35%** to 147,000, and **stock** was down almost **50%** to 130,000 by the end of Q1 2025.

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.

We would like to hear from you.

In Q2, we will be focusing on scraping and data harvesting. Whether you are a scraping service, have engaged scraping services or have been impacted in scraping - we want to hear from you. Reach out through the following options:

Email: team-threat-intel@kasada.io

Discord: kasadaiq

Twitter: @kasadaiq

How KasadaIQ can help:

- Unparalleled insights into the adversary ecosystem. Our collection consists of deep access across 2,000+ unique collection locations, with over 23 million messages ingested each month.
- Deep expertise on the automated threat landscape, adversary behaviour 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 behaviours and patterns.
- Threat reporting. We equip you with regular cadence reporting on relevant trends at the organisation and/or industry level, tailored for all levels of audiences across your organisation.