kasada

KasadaIQ

Quarterly Threat Intelligence Report

Q2 2026

Introduction

Kasada's Q2 2026 Threat Intelligence Report (Q2 Threat Report) provides contemporary observations and assessments to counter automated threats. Drawing on the millions of unique events collected by KasadaIQ each day, the report highlights key areas for organizational focus. All insights come from analysis and investigations by our in-house KasadaIQ intelligence capability, supported by extensive open and closed sources and decades of combined expertise.

Intelligence Requirements

01

What is the **quantifiable impact** of automated threats and what drives adversary behavior?

02

Who comprises the adversary landscape and what are their capabilities, motivations and organization?

03

How will the **threat landscape evolve** over 6-12 months and what emerging threats require preparation?

How To Read This Report

This report is designed to serve both analysts and executives. Strategic assessments and adversary insights provide the depth practitioners need, while key findings and data callouts are structured to support board-level briefings and risk conversations.

- Threat drivers, trends and adversary developments covered in this report are generally applicable across industries. Where a development is particularly relevant to a specific vertical, it is marked with the relevant industry icon.
- For industry-specific analysis, the Industry Breakdowns section translates the report's findings into per-industry views across accommodation, airlines, entertainment and ticketing, gaming, quick service restaurants, retail, social networks, streaming and webmail. Each breakdown surfaces the key data and applies the relevant threat drivers discussed throughout the report to that vertical, giving readers a focused view of what matters most for their organization.

Table of Contents

Executive Summary

Q2 2026 highlights a threat landscape accelerating in cost and velocity, rather than nature. Of 27 predictions tracked by KasadaIQ, **nine** evolved, with notable shifts in AI adoption, credential markets and bot economics. Ultimately, AI is reshaping adversary methods, not their motives or identities. Operations are becoming cheaper, criminal account markets are consolidating high-value inventory and major events continue to serve as lures for established tradecraft.

Threat Activity

11.7M+
Criminal Marketplace Stock
287.9K+ sales I **6K** active sellers

~77
Malicious Configurations
Target & enabler layers

20.9K+
Bot Checkouts
32+ brands I **8+** product categories

AI-Accelerated Threats

14K+
AI Account Sales
14.8K+ stock I **6** products

$7-$60
Per-Account Price
Shared to private, 1 to 12 months

11.3M+
AI Crawler Visits
Across **2** AI crawlers in **1** month

Adversary Economics

94%
Rent, Don't Build
Of classifiable adversaries

$400+
Cost to Operate
Fully equipped newcomer

$0.30/GB
Residential Proxies
IP no longer sorts traffic

Spotlight: The Psychology of a Fraud Enabler

Two operator cohorts (2018 and 2026), only capability differs. Motivation and rationalization hold to patterns documented for **70+** years.

Key Insights

AI is a speed change, not a population change.

KasadaIQ places the AI movement at the tooling layer, not the autonomous one. KasadaIQ did not observe any campaigns running without human orchestration, and OpenBullet is still the dominant credential-stuffing tool. The cost of capability is what collapsed, with an external demo defeating a commercial licensing system for $3.88 in under five hours. The Spotlight extends the same finding to the people: across two operator cohorts active since 2018 and arriving in 2026, motivation and rationalization are unchanged and only capability differs, consistent with drivers that have held for 70+ years. The how is changing fast; the who and the why are not.

Read more: Threat Drivers & Trends (AI as a force multiplier) and Spotlight: The Psychology of a Fraud Enabler.

The barrier to entry is increasingly financial over technical, and a core control is eroding.

Roughly 94% of classifiable operators rent capability rather than build it, and a newcomer is fully operational for $400 to $500 with no development of their own. Clean residential proxies now sell from $0.30/GB, so IP reputation no longer separates malicious traffic from legitimate. Solver-API services rent frontier bypass downmarket, compressing the capability gap even as the hard reverse-engineering stays exclusive.

Read more: Threat Drivers & Trends (Commoditization of attack infrastructure) and 2026 Prediction Tracking.

Major events are lures for standing tradecraft, not sources of new fraud.

World Cup activity tracked the official ticketing calendar rather than the match schedule, with inventory dormant until each on-sale then activating sharply. The tooling is year-round and reusable: KasadaIQ already holds a Rugby World Cup 2027 scalping playbook captured over a year early and built to the same template. External reporting frames the scale around the event (4,300+ fraudulent FIFA domains, 270,000+ credentials stolen, nearly 400 streaming domains seized), but the adversaries are the same ones who attach to whichever event comes next.

Read more: Threat Drivers & Trends (FIFA World Cup 2026).

Considerations for Defenders

Prioritize the **human-plus-AI risk surface**, since the immediate threat is humans re-tooling with AI at speed. The controls that hold raise the cost and reset the cadence of bypass through behavioral detection.

Break solutions faster than operators can re-rent them, because when ~94% rent rather than build, **frequent challenge resets** degrade service across the whole buyer tier.

Plan for **fraud enabling as a permanent condition**, because friction-only defenses fail when the work pays well, so the real leverage sits at the infrastructure, legal, and payment-rail layers.

Threat Landscape Update

Account Takeover Trends

287.9K+
Total Account Sales on Criminal Marketplaces

$1M+
Revenue from Criminal Marketplace Sales

~77
Malicious Configurations Ingested by KasadaIQ

6K+
Active Account Sellers

In Q2 2026, KasadaIQ tracked 6,076 active stores against 6,189 in Q1, a decline of **1.8%**. The turnover reflects churn, not collapse. Persistence was high, with **97.6%** of Q1 stores still trading in Q2, and the net loss of 113 stores resolves into 149 departures against 36 arrivals. Some of that turnover is host migration rather than genuine exit, so real churn is lower still. Against a stable seller population, the sharp decline in observed sales and stock cannot be attributed to the market contracting, and instead points to reallocation within the persistent cohort and a small number of high-volume dropouts. Average prices increased in most industries, indicating surviving inventory skewed toward higher-value accounts (see below). See Industry Breakdowns for further details.

Interpretation note: Kasada's Threat Intelligence collection methodology continues to evolve. New sources are added regularly, while older sources disappear due to legal takedowns, seller migration, and source exhaustion (credential supply drying up for a given seller or venue). Sales, stock and revenue are modeled from observed stock movement, exclude unlimited-stock listings, and should be read as directional rather than total.

Industry	Total Sales	Stores Selling Accounts	Maximum Available Stock	Revenue from Sales	Average Account Price
Accommodation	▼74%	▼16%	▼74%	▼59%	▲61%
Airlines	▼55%	▼13%	▼62%	▼78%	▼52%
Entertainment & Ticketing	▼16%	▼7%	▼30%	▲22%	▲46%
Finance	▼32%	▼44%	▼34%	▼61%	▼42%
Gaming	▼92%	▼8%	▼47%	▼39%	▲626%
Quick Service Restaurants	▼63%	▼1%	▼42%	▼53%	▲27%
Retail	0%	▲5%	▼50%	▲40%	▲40%
Social Networks	▼97%	0%	▼49%	▼92%	▲137%
Streaming	▼24%	▲5%	▼42%	▲67%	▲121%
Webmail	▼99%	▲2%	▼59%	▼96%	▲214%

MALICIOUS CONFIGURATIONS

KasadaIQ analyzed approximately **77** distinct configurations collected in Q2 2026, each classified by target. A configuration is a simple text file that instructs web automation tools (like OpenBullet) on how to generate HTTP requests against the target website or web application, execute browser commands and return data from accounts that have been successfully taken over. Configuration creators can develop highly sophisticated attacks by leveraging complex code structures that use diverse variables and functions. Once developed, these configurations are frequently circulated, traded or sold across criminal networks, enabling adversaries to execute large-scale credential stuffing or brute force campaigns against targeted websites.

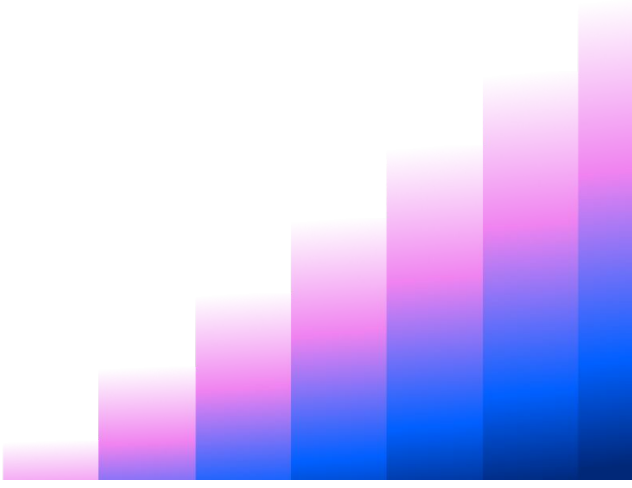
All figures represent observed tooling rather than total adversary activity. The most significant trend is a shift in target: while most configurations still exploit high-value accounts (gaming, streaming and retail), a separate cluster now targets the enabler layer (the proxy, identity, and masking services) that facilitate wider threats.

The Enabler Layer

Around **17%** of configurations targeted services that confer capability rather than resale value. The majority of these focused on illicit infrastructure that enables scalable phone verification bypass (proxy marketplaces, mining platforms, Telegram shops and SMS verification services). A smaller subset targeted VPNs, providing both resale value and operational masking. AI-adjacent tools also function as critical enablers, acting as both targets and automation mechanisms. This strategic investment in foundational infrastructure signifies a shift toward bolstering the capabilities that power broader credential-stuffing operations.

The Target Layer

Among configurations targeting accounts for their own value, Gaming was the single largest industry, accounting for **~16%**. Gaming accounts attract sustained attention for their resale value, stored payment methods, and in-game inventory, and several configurations captured account balance, owned titles and rank, the attributes that set a resale price. Streaming (**~13%**)and Retail (**~12%**) followed, characterized by opportunistic, broad-spectrum coverage across diverse brands rather than targeted attacks on specific entities. The spread points to opportunistic coverage rather than focus on one high-value brand.



AI Insights

In Q2, two primary factors shaped the AI threat landscape: a surge in automated traffic from AI crawlers and a consolidated market for reselling compromised AI accounts. Both trends stem from a common source: the increasing value of AI capabilities has incentivized adversaries to scrape content for model training and steal existing accounts to gain unauthorized access.

Resale Market

14,886+
Active listings in stock across **6** AI products

14,055+
AI account sales across the quarter

Automated Traffic

11.3M+
Requests from 2 AI crawlers in a single month

DEMAND: AUTOMATED TRAFFIC LOAD

AI-driven automated traffic is a distinct and growing load on customer properties. In a single month, KasadaIQ observed **11.3M+** requests from just two AI crawlers, ByteSpider and Meta (see below). That volume from only two operators shows how concentrated and heavy the scraping load has become, competing with legitimate traffic and harvesting content at a scale most properties are not provisioned to absorb. The same value that drives this scraping, access to AI capability, is what makes AI accounts worth stealing and reselling.

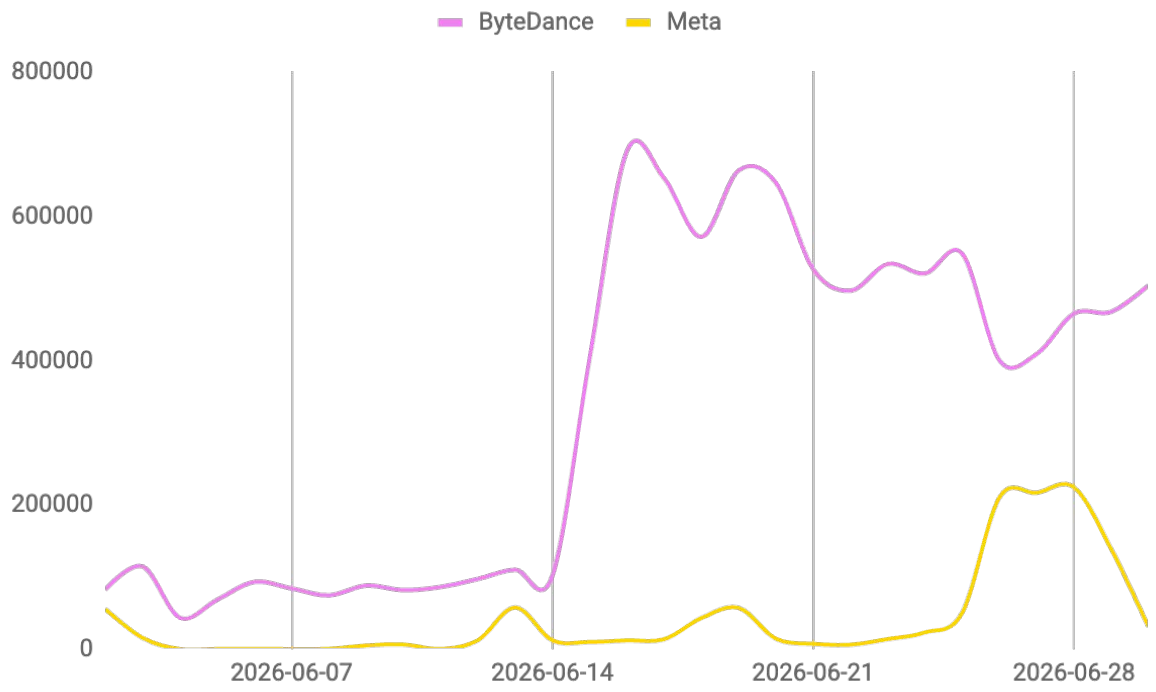


Chart 1. ByteSpider and Meta traffic by day (June 2026)

PRODUCTION: MALICIOUS CONFIGURATIONS

AI platforms are an established credential-stuffing target, not an emerging one. AI-targeting configurations have appeared in KasadaIQ collection every quarter since at least Q1 2023, with the defining wave in Q3 2023 occurring alongside ChatGPT's mass adoption. Of the 77 Q2 configurations, **12%** targeted AI platforms, placing it on level with the retail industry.

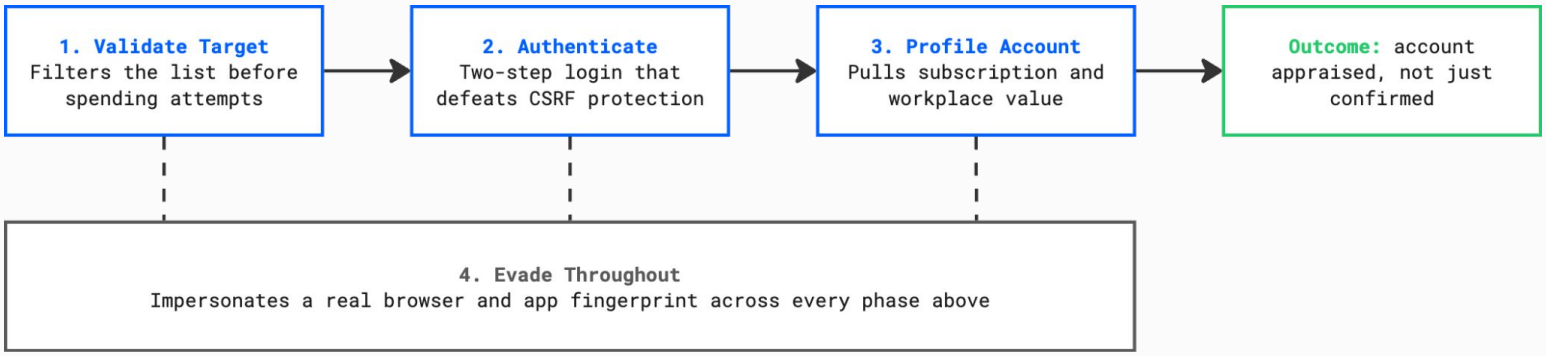
What distinguishes the Q2 configurations is not that they target, but what they extract. Of the nine AI-targeting configurations, three carry detailed capture schemas revealing intent. Each instruments for a different form of account value:

1. Generation credit balances, treating the account as a wallet of prepaid compute to be drained.
2. Paying and business-account status, grading the account for resale value.
3. A full account profile spanning two-factor status, subscriber tier, trial eligibility, employee flag and follower reach, harvested to value and triage the account for takeover (see below).

Snapshot: AI config capture schema

One AI-targeting configuration alone captured 24 distinct account fields on login, including subscriber type, trial days remaining, free-trial eligibility, two-factor status, region, employee flag and follower counts. It was the most complex configuration observed in Q2 collection, and its capture schema was a direct inventory of what the operator intends to harvest.

The diagram below abstracts that configuration into its four functional phases. It moves through them in sequence, validating each target before spending an attempt, completing a login that works around the platform's anti-forgery protection, and then pivoting to the platform's own internal interfaces to pull subscription and workspace data, while impersonating a legitimate browser throughout.



The final phase is what distinguishes this configuration from a standard credential checker. A checker stops once it confirms a login is valid; this configuration continues, retrieving the account's subscription tier, trial status and stored value. It does not just confirm access, it appraises the account, harvesting the same attributes that determine a listing's price on the resale market. The capture schema is a valuation rubric, and it is the clearest single illustration of how the tooling layer feeds the account trade.

Beyond account theft, Q2 saw rising abuse of AI-adjacent tools, such as virtual SMS services for bulk account creation. AI now functions as both a target and an enabler; while Q1 focused on the AI account market, Q2 reveals the supply-side tooling used to produce and value them. These capture schemas demonstrate clear intent and capability, though this analysis does not quantify actual theft.

DISTRIBUTION: THE RESALE MARKET

In the Q1 2026 Quarterly Threat Report, KasadaIQ reported a **640x** increase in daily paid AI account sales compared to Q4 2025. Q2 shows that surge was not a single-quarter spike. The trade has consolidated into a steady, high-volume market, with **14,055+** AI account sales across the quarter and **14,886+** active listings in stock across six products.

ChatGPT drives a majority of this activity. Plus, Pro and Team subscriptions account for **13,140** of Q2's sales and **12,850** of in-stock listings, roughly **94% of AI-account sales** and **86% of AI-account inventory**. ChatGPT combines the largest paid install base, and therefore the deepest pool of both compromised accounts and buyers seeking them. It has the steepest price arbitrage at its $100 and $200 Pro tiers. Its payment and regional restrictions push buyers toward illicit access, while its ubiquity keeps it surfacing in infostealer logs far more often than other products.

Perplexity is the notable secondary target, with around **2,100** accounts and vouchers observed. Most of these are voucher or redeem codes rather than pre-made shared accounts, which points to voucher code abuse or payment method fraud rather than straightforward credential theft. The voucher model appeals to buyers because it lets them upgrade an account they already control rather than share a compromised login. Adversaries align their instrumentation with each product's specific monetization model, mirroring patterns observed in the configuration data. KasadaIQ assesses this pattern will grow wherever subscription products issue redeemable codes.

Pricing runs from $7 to $60 per unit, scaling with access type (from shared through to private) and duration (from one month to one year). Longer subscriptions dominate, with three, six and twelve-month plans outselling monthly.

Automated Checkout Activity

20.9K+
Total Bot Checkouts Observed

380
Average Daily Bot Checkouts

32+
Brands Targeted in Bot Checkouts

8+
Product Categories Targeted in Bot Checkouts

THEME 1 **BOT CHECKOUT TIMING**

In Q2, bot checkout activity was heavily drop-driven. Looking at total bot checkouts by day (see right), Monday through Wednesday are the primary drop days, with Wednesday the clear peak at an average of **742** checkouts, more than double any other day. Weekends are quieter, with Saturday and Sunday accounting for only around 11% combined. Activity concentrated sharply on a handful of drop dates: the three busiest days all fell in mid-April (April 13 to 15), driven almost entirely by high-profile sneaker releases.

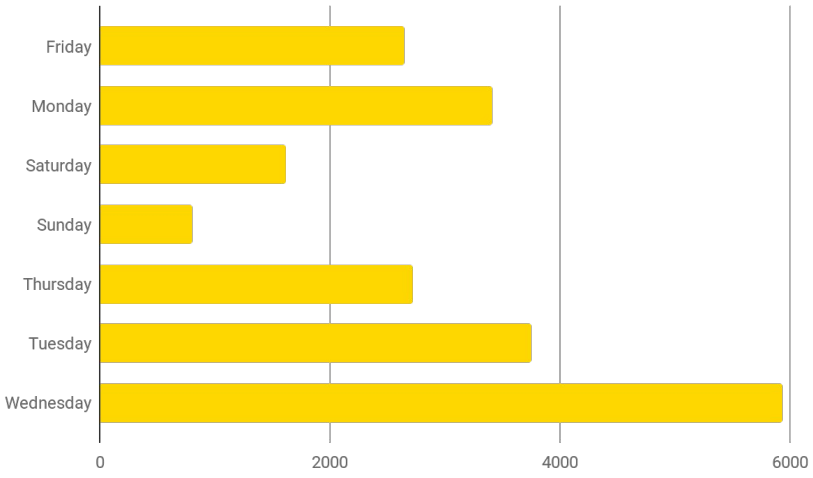


Chart 2. Bot Checkouts by Day in Q2 2026 (Apr-June)

Bot activity is release-driven, clustering during scheduled midweek sneaker drops rather than following steady daily demand or seasonal trends.

THEME 2 **BOTTERS DIVERSIFYING TARGET ITEMS**

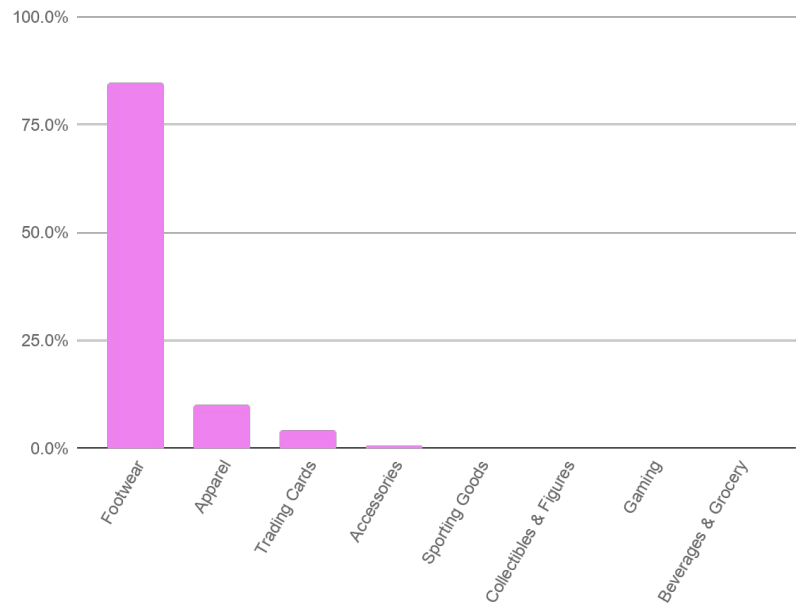


Chart 3. % of Bot Checkouts by Product Category in Q2 2026 (Apr-June)

In Q2, KasadaIQ observed successful bot checkouts across **8+** unique product types (see left). Footwear dominates, but apparel and trading cards are the real secondary targets. Footwear constitutes **84%** of checkouts, apparel **10%** and trading cards **4%**. Trading cards are a coordinated secondary vertical worth flagging. Sealed trading card product is a known bot-and-flip target, and its presence (**899** checkouts across **8** brands) shows the same automation pointed at TCG releases as seen in footwear.

2026 Prediction Tracking

9 of 27 predictions moved this quarter, with none refuted.

Full list of predictions is at [Appendix 1](#).

TRACKED	MOVED	HELD STEADY	REFUTED
27	9	18	0

●●●● Occurring 5

RES-07 ●●●●
Scalpers shift focus to less regulated Items

ENA-04 ●●●●
Low forum mentions indicate bot success

ENA-05 ●●●●
Malicious ASNs prevail

ENA-06 ●●●●
IP reputation collapses

ATO-02 ●●●●
Credential packages expand

●●●○ Partially 8

AI-01 ●●●○
AI-native adversaries emerge (see **here**).

AI-03 ●●●○
Bot operators overcome AI scepticism

AI-09 ●●●○
Block v. allow dilemma intensifies

AI-10 ●●●○
Legal precedents lag behind technology

ATO-01 ●●●○
'Fresh credential' marketplaces emerge

RES-01 ●●●○
AI-generated 'social proof' expands

RES-03 ●●●○
TikTok Shop as major fraud surface

RES-04 ●●●○
Social capital as a key driver for reselling

●●○○ Starting 10

AI-02 ●●○○
AI v. AI arms race

AI-04 ●●○○
Novices build working bots using AI

AI-06 ●●○○
Server-side AI monitoring

AI-07 ●●○○
AI agents replace single massive traffic spikes

AI-08 ●●○○
Gray area AI-driven shopping research

ATO-03 ●●○○
AI-powered credential stuffing grows

ATO-05
Credential-to-cash conversion times drop

RES-05 ●●○○
Scalpers employ more sophisticated bots

ENA-02 ●●○○
Barrier to bot ops is financial › technical

ENA-03 ●●○○
Gap widens between budget & funded ops

●○○○ Early signs 3

RES-02 ●○○○
'Flash scalping' operations emerge

RES-06 ●○○○
Regulatory crackdowns push underground

ATO-04 ●○○○
Cross-platform credential correlation

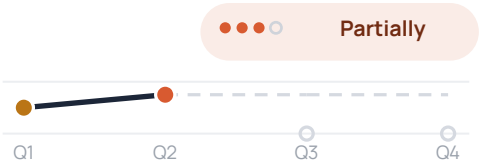
○○○○ Not observed 1

AI-05 ○○○○
AI automates raffle entry

WHAT MOVED THIS QUARTER (1/2)

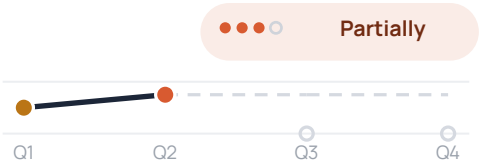
AI-03 Bot operators overcome AI scepticism

Q1–Q2 2026 evidence confirms adversaries are scaling AI operations, with isolated examples of genuinely autonomous pipelines. However, the dominant pattern for adversaries tracked by KasadaIQ remains AI-augmented human operators. See Threat Drivers & Trends.



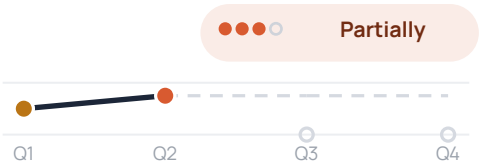
AI-09 Block v. allow dilemma intensifies

5+ independent sources documented a Q1–Q2 2026 shift to industrial-scale AI operationalization among adversaries. Discord community sentiment shows majority of ecosystem focus is on usage (19%) and capability (14%). See Threat Drivers & Trends.



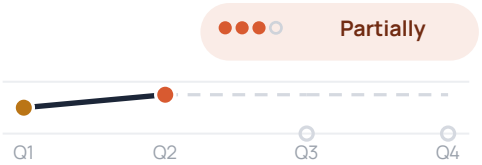
ATO-01 'Fresh credential' marketplaces emerge

4+ independent sources corroborate value-tiered credential selling activity. In monitored communities, KasadaIQ observed structured, tiered credential markets with an emphasis on account value. Freshness and session-data tiering were smaller and more specialized segments. See Threat Drivers & Trends.



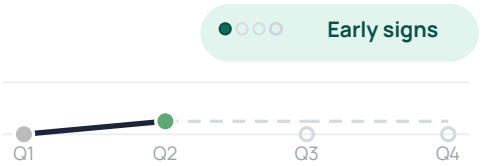
RES-01 AI-generated 'social proof' expands

Documented with named real-world cases, confirming the expansion of AI-generated social proof beyond fake reviews. The phenomenon is monetized, productized and operating at scale. The nuance is that highest-volume documented abuse is currently concentrated in specific verticals (wellness, adult content, affiliate fraud) rather than saturating all eCommerce social proof, so it is occurring and growing rather than universal.



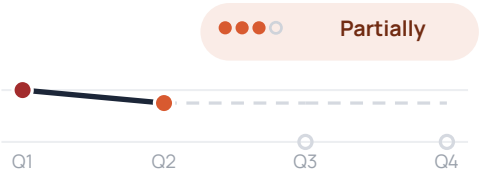
RES-02 'Flash scalping' operations emerge

AI detecting social-driven demand trends) is real and mainstream, but it's deployed by the legitimate side (retailers anticipating demand, resellers sourcing and pricing). In Q2, new services and research emerged indicated growing consumer demand for this kind of AI-based tooling that directly links social media trends to product research.



RES-04 Social capital as a key driver for reselling

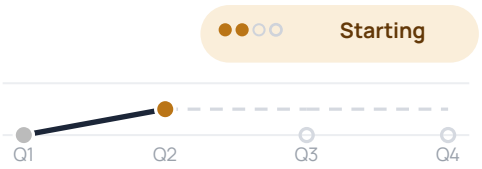
This quarter's evidence pulls RES-04 back from Occurring to Partially Occurring. The earlier call assumed virality was driving target selection, but on closer collection the signal is concentrated where reselling communities plan drops, not where they transact: it spikes in agenda and onboarding channels (around 90% in one community) and falls to lower proportions in the trade and checkout channels. That pattern shows virality is a topic operators watch and discuss, not yet a proven trigger for what they target, which is the gap that justifies the downgrade.



WHAT MOVED THIS QUARTER (2/2)

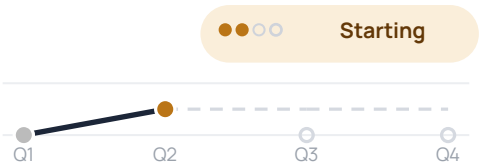
ENA-02 `Barrier to bot ops is financial > technical`

Of users classified by KasadaIQ, roughly 94% are buyers of tooling. A newcomer can stand up a working operation for about $400 to $500. Newcomer questions stayed a small share of all messages through the half, ticking up to a May high of 0.8% before easing in June, so the funnel is widening modestly rather than surging. See Threat Drivers & Trends.



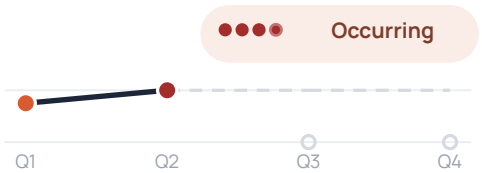
ENA-03 `Gap widens between budget & funded ops`

The stratification is real and both tiers are clearly present in collection. However, the "gap widens" framing is too simple: the dominant dynamic is commoditization, solver-API services package the sophisticated tier's bypass work and rent it cheaply downmarket, compressing the capability gap on established defenses even as frontier reverse-engineering stays exclusive.



ENA-06 `IP reputation collapses`

Multiple competing vendors now sell residential bandwidth below $1 per gigabyte. They compete on exactly the attributes that defeat reputation scoring: one markets "clean, low fraud score, bulk, undetectable" and another advertises "clean proxy delivery". See Threat Drivers & Trends.



Threat Drivers & Trends

The Threat Landscape Update quantifies what KasadaIQ observed this quarter; Threat Drivers & Trends explain the forces behind those numbers. Each driver pairs external corroboration from open sources with KasadaIQ's own collection and tooling review, and each connects to one or more of KasadaIQ's 27 predictions for 2026.

AI: force multiplier, not autonomous adversary

Connected Predictions: AI-01, AI-02, AI-03, ATO-03

KasadaIQ collection and external reporting show a shift from AI-assisted to AI-operationalized attack pipelines. KasadaIQ places the reality at the tooling layer rather than the autonomous one. KasadaIQ did not observe any campaigns running without a human in the loop; the "fully automated" language describes component-level automation with an operator still orchestrating. While external reporting documented a push toward autonomous operation (like University of Toronto's self-replicating worm proof-of-concept), KasadaIQ has not observed this trend in the automated threat landscape to the same extent.

KasadaIQ Observations:

- While online communities are heavily focused on AI, they have yet to adopt it for operationally critical tasks. OpenBullet remains the dominant tool for credential stuffing.
- Users are developing techniques to coerce AI through prompt injection and jailbreaks to generate bypass and reverse-engineering code. There is also an emerging market for "jailbroken" accounts, such as Claude instances with security guardrails removed.
- The 2025 FBI Internet Crime Report documented ~$900 million in AI-related scam losses due to the proliferation of difficult-to-detect synthetic content.
- Researchers demonstrated how AI models can be used to reverse-engineer tooling (see Case Snapshot below).

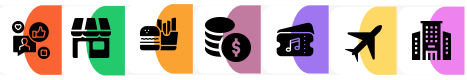
CASE SNAPSHOT: SOFTWARE LICENSING SYSTEM DEFEATED FOR $3.88

In a public demonstration, open source researchers showed how a commercial AI model could reverse-engineer a piece of protected software and defeat its licensing system in under five hours, for $3.88 in API credits. The work ran on a maturing open source toolchain that wires AI directly into reverse-engineering platforms, with projects like GhidraMCP and ida-pro-mcp each drawing thousands of users. The model did the grinding analytical work a skilled human would otherwise spend days on but a person still framed the task, pointed the tooling and used the result.

Analyst Comment:

The immediate threat is not autonomous AI, but humans leveraging AI to re-tool against defenses at unprecedented speed and lower cost. The most effective controls are still the ones that raise the cost and reset the cadence of bypass, behavioral detection and challenge integrity. Until config-less credential stuffing replaces current tooling, prioritize the human+AI risk surface.

Agentic commerce as an emerging attack surface



Connected Predictions: AI-03, AI-07, AI-08, AI-09

Verified AI-agent traffic is growing slowly but remains marginal, showing no signs of displacing normal traffic. While KasadaIQ expects growth, the industry lacks consensus on defining and handling authorized agent activity, and operator interest remains driven by trend-following rather than operational necessity.

KasadaIQ Observations:

- Agentic commerce updates from Google, Shopify and Anthropic signal mainstream adoption. Researchers turned a popular AI browser into a working phishing scam in under four minutes.
- The Amazon v. Perplexity appeal has reached the Ninth Circuit, where arguments on June 11 questioned whether the *Computer Fraud and Abuse Act* applies to AI agents.

Analyst Comment:

Agentic commerce is low-volume yet high-consequence; acting with full customer authority, a single compromised agent causes more damage than a wave of standard bots. The Amazon v. Perplexity outcome will legally define authorized activity and signal shifts in corporate obligations.

Commoditization of attack infrastructure

Connected Predictions: ATO-01, AI-02, ENA-02, ENA-03, ENA-05, ENA-06

The bot economy runs on rented capability. Of the operators KasadaIQ could classify, the overwhelming majority (**~94%**) buy what they need rather than build it. A newcomer can be fully operational for a few hundred dollars with no development of their own. Underneath sits a thin frontier tier (produces the hard capability, proxies, bypass and credentials) and a services layer (rents it downmarket as cheap, off-the-shelf product).

KasadaIQ Observations:

- A newcomer can be operational for $400-500 with no development of their own. Going rates are attainable, with a bot license around $350, a subscription around $25, accounts around $50 and proxies under a dollar a gigabyte.
- The proxy market commercializes evasion, even utilizing sanctioned infrastructure. Vendors sell "clean" residential proxies for as low as $0.30/GB.
- Researchers showed how BrightData's iOS SDK embedded in consumer applications turns a user's phone or smart TV into an exit node for web scraping traffic sold on to the AI industry. While user consent is technically present, it is not well informed and nor delivered in a user friendly way.
- Advanced bypass methods are commoditized through Solver-API subscriptions. Due to the high engineering costs of custom maintenance, most adversaries rent enterprise evasion tools instead of building them.

Analyst Comment:

Since most adversaries rent rather than build bypass capabilities, economic leverage lies in breaking solutions faster than they can be re-rented. Frequent challenge resets increase the maintenance burden on sellers, rendering off-the-shelf products obsolete and degrading service across the entire buyer tier.

FIFA World Cup 2026: a lure for standing tradecraft

Connected Predictions: RES-02, RES-04, RES-05, RES-06

The FIFA World Cup 2026 is the kind of concentrated, high-demand event that historically draws scalping and fraud. External reporting reflects that expectation across several vectors. The FBI's IC3 warned that adversaries are spoofing FIFA websites through typosquatted domains to harvest personal data and sell fake tickets and hospitality products. Group-IB tracked more than 4,300 fraudulent FIFA domains since August 2025, including a campaign dubbed Ghost Stadium that cloned FIFA's login system and stole over 270,000 fan credentials. Proofpoint found that more than one third of official World Cup commercial partners lacked the strictest DMARC enforcement, leaving fans exposed to spoofed emails. In late June, the US Department of Justice (US DOJ) seized nearly 400 domains used to illegally stream World Cup matches under Operation Offsides.

KasadaIQ collection showed a consistent pattern beneath this activity. Adversary activity around the World Cup tracks the official ticketing calendar rather than the match calendar. Inventory stayed dormant until a sales milestone, then activated sharply, with supply, reselling and cashout following in sequence as each official on-sale opened. The published sales-phase schedule functioned as an early warning indicator, and the first-come-first-served final phase marked the peak threat window. Observed adversary activity spanned a range of threat types but stayed modest in distinct volume, and it runs on standing tradecraft that adversaries redirect toward whichever major event comes next. The tournament serves as a lure on existing fraud rather than a source of new fraud.

KasadaIQ Observations:

KasadaIQ tracked adversaries following the FIFA ticketing lifecycle in three phases (see chart below). From January 2026, activity ran at a steady baseline dominated by account stock with supply gathering ahead of demand. This baseline collapsed in late March, coinciding with qualification concluding (March 31) and the prior sales phase closing. Activity then rebuilt and broadened from mid-April, with reselling & ticket scalping and streaming piracy surging alongside FIFA's Last-Minute Sales Phase (April 1) and Resale Marketplace (April 2) openings, and climbing towards the kickoff (June 11).

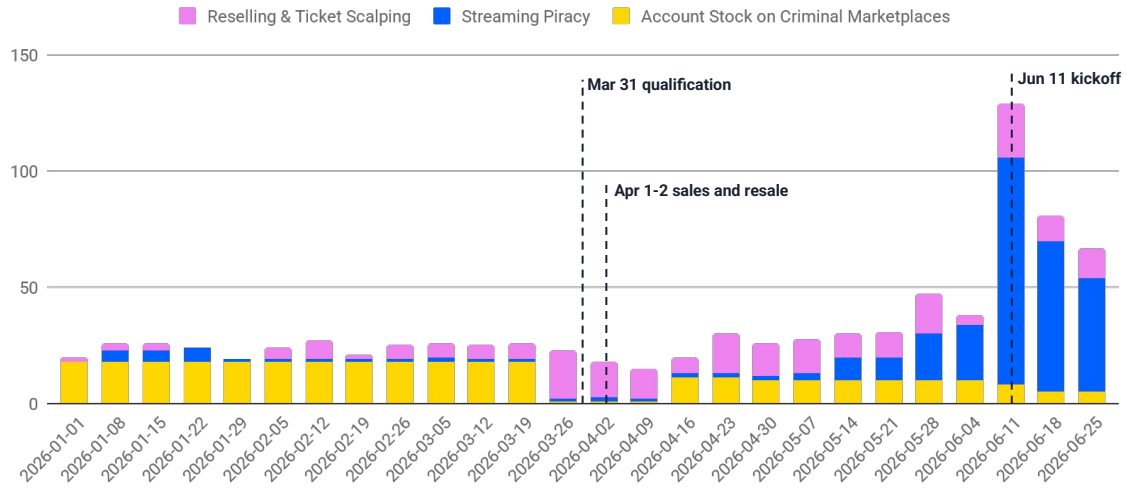


Chart 4. Weekly World Cup threat activity by threat type (Jan-June 2026)

The chart above reliably shows timing and sequence. The bands draw on different measures, so they read best as trends rather than like-for-like totals. Streaming piracy's prominence on the chart is conflated by amplification, those 212 distinct messages repost to nearly 12,000 appearances, so its mid-April-to-June bulk reflects heavy reposting rather than a proportional rise in operators.

KasadaIQ observed a number of different threats in our collection, described below.

Streaming Piracy	KasadaIQ observed at least 13 distinct IPTV services advertising World Cup streaming, one forum guide describing an IPTV reselling operation claiming $70,000 a month and a handful of marketplace access listings. This sits inside a much larger ecosystem evidenced by the US DOJ's Operation Offsides. Illicit streaming is a known delivery vector for credential theft and malware, so fan demand for free matches funnels victims toward infrastructure that feeds the account-compromise supply chain Kasada's customers face.
Reselling & Ticket Scalping	KasadaIQ identified significant World Cup-related reselling. Ticket scalping involved up to 150 listings, featuring venue-aware routing, fee analysis across platforms like FIFA Marketplace and Viagogo, and organized, match-specific playbooks for queue evasion. Simultaneously, automated-buying communities (typically targeting sneakers and collectibles) exploited merchandise like trading cards, LEGO sets and licensed apparel, treating the tournament as a major retail event.
Account and Profile Sales	Adversaries sold FIFA ballot entries and account-generation services ("acc gen + entry, private script, won on all previous ballots") priced on bulk stolen-credential inputs (advertised at a minimum of 2,000 cards and 2,000 emails), queue passes ("selling queue passes during fifa, dm to get on list"), and pre-made FIFA accounts. The scalping playbook mentioned above reinforced this layer, instructing buyers to pre-create FIFA accounts and run 15 to 20 Chrome profiles to hold multiple queue positions.
Other	KasadaIQ identified a claimed European football organization breach impacting 45,000-plus players and officials (license numbers, FIFA IDs, names, birth dates). Vendor-asserted, scope unverified. Separately, a service marketed via FIFA's 2025 heritage-document fraud scandal, linking the World Cup activity to the standing KYC-bypass market.

Analyst Comment:

The World Cup did not create a new wave of fraud. KasadaIQ's observations relate to established, year-round adversary tradecraft attaching itself to whichever major event is next, with the tournament as cover. Collection already holds a Rugby World Cup 2027 scalping playbook captured over a year ahead and built to the same template as the FIFA one, showing operators preparing for the next target well in advance. Because the threat is standing rather than event-specific, the most reliable warning signs come from the adversaries'' own rhythms. Criminal activity tracks the official ticketing calendar rather than the match schedule, so the sales-phase calendar shows when to pre-stage controls, with the first-come-first-served final sale the highest-threat moment. A structured release analysis carries its own warning, marking the point at which adversaries commit to a named event and setting out their target matches and resale venues in advance. Monitoring both across all major sporting events anticipates the threat earlier than investigating each tournament on its own.

Spotlight: The Psychology of a Fraud Enabler

Q2's Threat Drivers & Trends were focused on AI as a force multiplier, agentic commerce, commoditized attack infrastructure and World Cup-related lures. While these trends reflect shifting capabilities and opportunities, the human element remains constant; every driver is a deliberate choice by a fraud operator. This section examines AI's true impact on the fraud ecosystem: what it has changed and what remains untouched.

Cybersecurity gets treated as a technology problem. The attacks are technical, the defenses are technical and the vendor language is technical. However, the ultimate decision to attack is made by a human. KasadaIQ's work this quarter has focused on what AI is actually changing about the population of fraud enablers and what it is leaving untouched. **The short answer is that AI is changing the how, not the who or the why.**

Despite major technical developments, the driving forces behind humans deciding to engage in fraudulent activity have remained relatively unchanged for **70+ years** .

A Fraud Enabler Diamond

In his 1953 publication, *Other People's Money: A Study in the Social Psychology of Embezzlement,* criminologist Donald Cressey asserted that the decision to commit fraud is heavily driven by conditional environmental and psychological factors. Developed through interviews with 133 inmates convicted of fraud-related offences, Cressey's Fraud Triangle found the simultaneous presence of three elements drove the human decision to engage in fraud:

1. **Pressure:** A non-shareable problem the person cannot resolve through legitimate means.
2. **Opportunity:** Perceived access to a way of resolving the problem covertly, using a position of trust.
3. **Rationalization:** A framing the person uses to reconcile the act with their self-image as a non-criminal.

Subsequent fraud literature has built on Cressey's original Fraud Triangle. In 1984, Albrecht, Howe & Romney broadened the framing of "pressure" to include financial, vices (like gambling), work-related and other personal pressures. In 2004, Wolfe & Hermanson added capability as a fourth element to capture skill, intelligence and confidence to execute and sustain the act. In 2011, Crowe Howarth added arrogance (also referenced as competence) as a fifth element, capturing the person's belief that controls do not apply to them. In 2019, Vousinas added collusion as a sixth element, arguing that modern fraud requires coordination between multiple parties.

These extensions were built to explain the behaviour of those directly committing the fraud. Fraud enablers are different as they do not commit the fraud themselves; they build and sell the capability that allows others to. Their relationship to the victim is not one of betrayed trust but of commercial supply. What the existing literature provides is not a model that applies cleanly to enablers, but the right set of ingredients to build one. Pressure, opportunity, rationalization, capability, arrogance and collusion are all present in the fraud enabler context, but each needs to be reframed for an external, commercial, networked operator rather than an internal, trusted, individual one.

KasadaIQ has adapted the elements the fraud literature has converged on into the Fraud Enabler Diamond (see below). Cressey's original three conditions have held for 70+ years; later work added capability (2004) and further elements through 2019. The Diamond retains four of these (motivation, opportunity, capability, and rationalization), contextualized for an external operator.

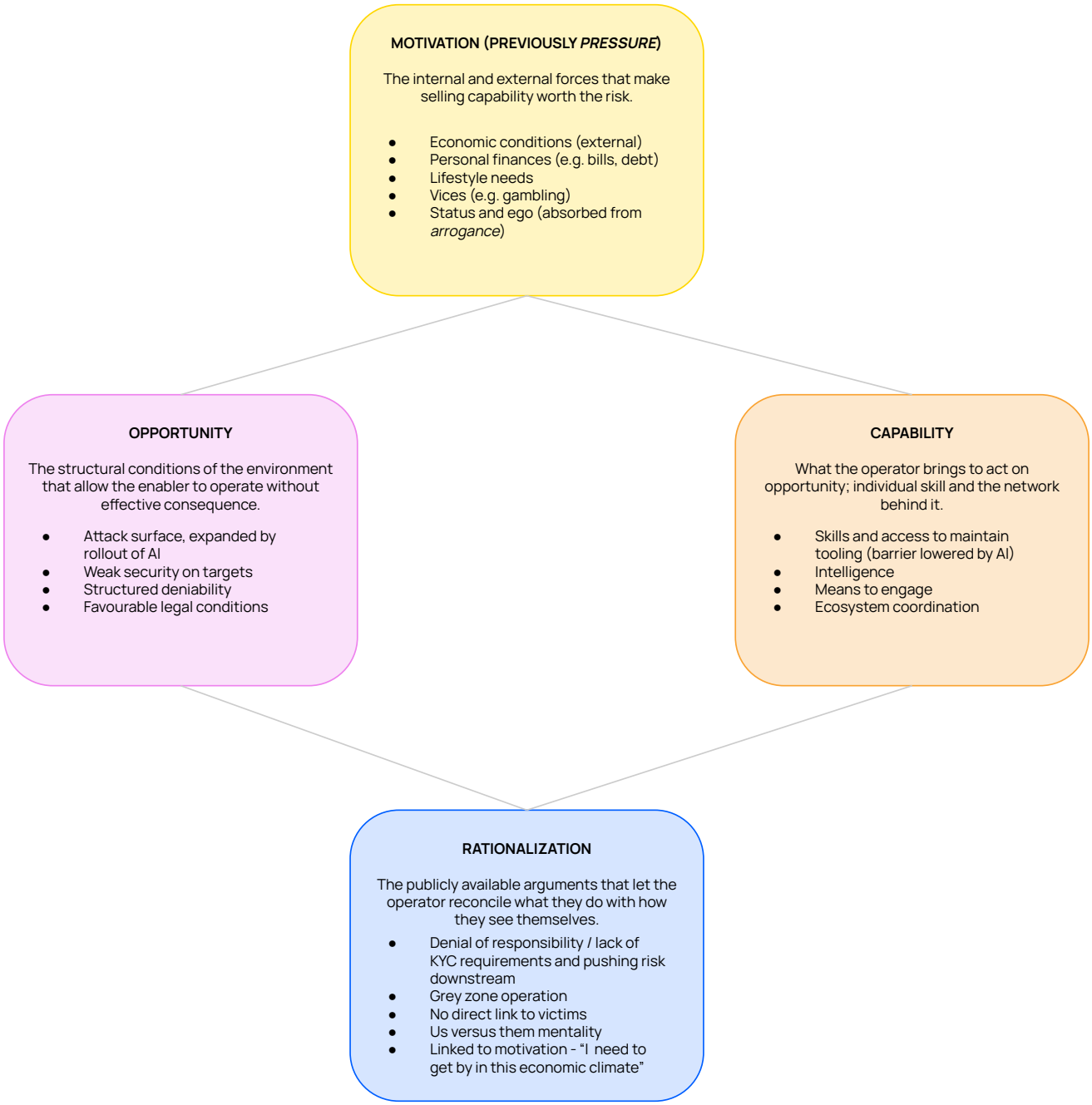


Figure 1. The Fraud Enabler Diamond

Pressure becomes motivation, capturing the sustained, self-directed combination of economic conditions, personal finances, lifestyle costs, and status that make selling capability worth the risk. Opportunity becomes the structural conditions of the ecosystem itself: a widening attack surface, weak security on targets, structured deniability, and favorable legal conditions. Capability covers individual skill, intelligence, means to engage, and the ecosystem coordination an operator can draw on. Rationalization becomes disclaimer architecture: a productized, publicly available system of arguments that lets the operator reconcile what they do with how they see themselves.

What the Diamond Surfaces

KasadaIQ monitors an online developer community and marketplace focused on automation, antibot bypass and scraping infrastructure which we will refer to as Shadow Stack. Shadow Stack has been active since at least 2018 and has 15,000+ members, of which around 20% actively engage. Its members swap techniques, code and tooling, making it a core environment for adversary capability distribution and uplift. Engagement since January 1, 2026 has concentrated on three themes: AI (**~24%**), anti-bot (**~20%**) and monetization (**~13%**), with KYC verification and tradecraft also visible (see right).

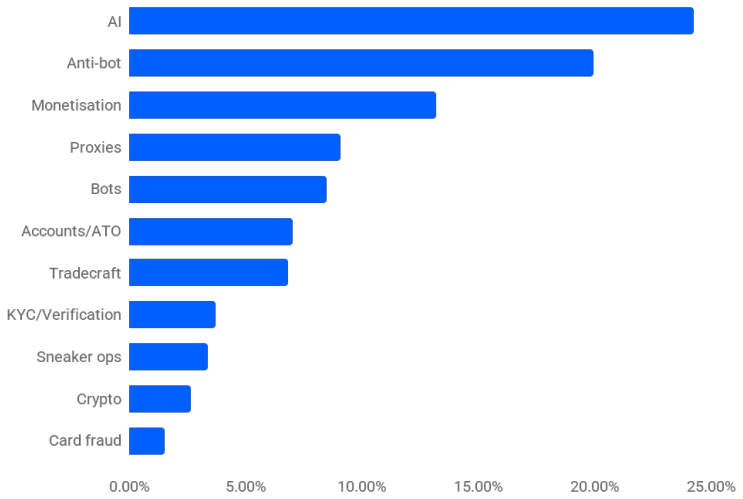


Chart 5. % of thematic focus in community activity

KasadaIQ's activity analysis shows two distinct adversary profiles operating within Shadow Stack. The *Established Cohort* has been active in the community for years. The *Emerging Cohort* has been enabled by vide coding and the broader expansion of LLM-assisted development. Both are examined below against the four elements of the Fraud Enabler Diamond.

	ESTABLISHED COHORT	EMERGING COHORT
Overview	• Long-tenured operators active in Shadow Stack since 2018-2019. • Top contributors produce an average of up to 40 messages per day. • Predominantly male, US-based. • Only a small minority are openly pro-AI. • Vocal inside the community but with limited external visibility. • Typically active in one or two communities.	• Have monitored the community in silence for up to a year but only started engaging in 2026. • Averaging 2-3 messages a day but posting is sporadic more than regular. • Predominantly male, US-based. • Openly pro-AI. • Maintain a loud and unambiguous public persona. • Active across multiple communities.
Motivation *The internal and external forces that make selling capability worth the risk*	• Sustained commercial activity over 5-7 years implies stable economic and lifestyle drivers; users claim their services pay for their rent and more. • Status and ego are signalled internally to peers rather than externally to the market, consistent with the cohort's deliberate OPSEC posture. • Community attachment functions as a non-financial driver.	• Motivation is explicitly making lots of money. • Openly disregards "good will" and society. • Often anchored in a determinist or anti-establishment philosophical position. • "Me versus the world" mentality. • Status and ego externalised through self-branding.

	ESTABLISHED COHORT	EMERGING COHORT
Opportunity *The structural conditions of the environment that allow the enabler to operate without effective consequence*	• Operates within an attack surface that has expanded materially with enterprise adoption of agentic AI. • Continues to exploit established attack surfaces (anti-bot, account creation, scraping) where the cohort has years of accumulated knowledge of defender behaviour. • Slower to pivot to agentic AI as an attack surface, consistent with the cohort's broader AI skepticism and preference for proven domains. • Favourable legal conditions and structured deniability sustained through quieter channels and embedded community relationships.	• Operates within the same expanded attack surface with the same structural conditions as the *Established Cohort*, but actively orients towards the newer agentic AI surface as a primary opportunity. • Market across multiple surfaces with cross-linked identities (commercial domains, brand-fronted entities, online communities, GitHub and X).
Capability *What the operator brings to act on opportunity; individual skill and the network behind it.*	• Deep individual technical capability acquired through extended practice rather than tooling assistance. • AI is not a primary input to capability acquisition or production. • Hold the line that there is far more to coding beyond what AI can do for someone. • High ecosystem coordination internally. Embedded community presence built over years of trust, with long standing lurker-to-contributor pathways. • Network capability narrow in reach, typically across one or two communities.	• Technical capability is often overstated. • High output but built on LLM-assisted development rather than years of practice, consistent with the broader vibe coding pattern. • Tooling already targets the seam where AI meets verification: vision-model solvers for image CAPTCHAs, browser automation that defeats behavioural anti-bot systems, and account creation flows that combine AI-generated identity material with device anchoring to defeat identity verification. • Network capability wider but shallower than the *Established Cohort*. • Multi-community presence but not well established. • Monitors adjacent communities for recurring pain points and builds tooling against them.

	ESTABLISHED COHORT	EMERGING COHORT

Rationalization
 	
The publicly available arguments that let the operator reconcile what they do with how they see themselves
	• Disclaimer architecture is refined through years of iteration.
	  ○ Code layer: tooling reframed as testing, research or education use.
	  ○ Commercial layer: customer interactions structured around plausible deniability rather than explicit acknowledgement of downstream use.
	  ○ Marketplace layer: positioning sustained quietly within trusted communities.
	• KYC absence framed as structural feature of the trade rather than operator choice.
	• Industry versus "Us" mentality. Gamified back and forth with the defender community.
	• Operator-victim distance maintained through layered tooling-not-action framing: the operator sells capability not outcomes.
	• Durable but less publicly visible than in the *Emerging Cohort*.
		• Disclaimer architecture is explicit, publicly documented and still being constructed.
		  ○ Code and commercial layers compressed into brand frontage. The cohort presents the work as legitimate data services rather than offensive tooling. Grey zone framing reinforced through commercial frontage.
		  ○ Marketplace layer: responsibility actively framed as belonging to the buyer or downstream victim.
		• Lack of KYC requirements on enabler-to-enabler transactions used to push compliance risk downstream.
		• Cites personal hardship and societal barriers as justifications, looping back to motivation as mutually reinforcing.

While the *Established* and *Emerging* cohorts share motivations (economic pressure, status, and self-justification through similar disclaimers), they differ in capability. The *Established* cohort relies on deep technical skill and high-trust networks, whereas the Emerging cohort leverages LLM-assisted output and broad, shallow community engagement. AI is expanding opportunity and shifting capabilities, but the core psychological drivers remain unchanged across operators active since 2018 and those appearing in 2026.

What This Means for Defenders

1 **Plan for fraud enabling as a permanent operating condition.** The conditions that produce fraud enablers have been the same for 70 years. Cost-of-living pressure, demand from a growing cybercrime economy, and visible KYC failures all point in the direction that produces more enablers, not fewer. Enforcement action, platform tightening, and defensive technology do not reset the population to zero. Treat enabler activity as a long-term business risk with sustained budget, not as an incident class that can be eliminated.

2 **Friction-only defenses fail when the work pays well.** Shadow Stack operators claim that a single bot rental can cover rent and more, and frame five and six-figure legitimate tech jobs as not worth their time. Most defensive strategies assume that enough friction will make operators give up, and this assumption only holds when the job is barely worth doing. When the job pays well, friction gets absorbed as a cost of doing business. Reducing enabler activity requires either making the work genuinely expensive at the infrastructure or legal layer, or cutting off how operators get paid through payment rails and marketplaces.

3 **AI changes how fraud enablers work, not who they are or why they do it.** The industry is talking about AI as if it has produced a new kind of adversary. KasadaIQ's monitoring indicates this is not the case. The people entering the market today are recognizable as the same kind of operator Cressey was describing in 1953, only with faster tooling and a wider attack surface. Defenders who calibrate to either cohort's tooling will miss the next one. Defenders who calibrate to the motivation and rationalization driving both will not.

Conclusion

The decision to engage in fraud has been driven by the same three conditions for over 70 years. This report adapts that framework into the Fraud Enabler Diamond, a four-element model for the external operator who builds and sells capability to the criminal economy. Applied against KasadaIQ's monitoring of Shadow Stack, the Fraud Enabler Diamond surfaces two distinct adversary profiles converging on motivation and rationalization but diverging on capability.

The central finding is that AI has changed how fraud enablers work, but not who they are or why they do it. The people entering the market are recognisable as the same kind of person Cressey was describing in 1953, only with faster tooling and a wider attack surface. Defenders should plan for fraud enablers as a permanent threat, take away the rationalizations that recruit the next cohort, recognise that the work is profitable enough to absorb friction rather than collapse under it and treat AI as a speed change rather than a population change.

Industry Breakdowns

ACCOMMODATION

THREAT: **ACCOUNT TAKEOVER**

Observed accommodation sales fell to 5,719 accounts (**-74.3%**), while revenue dropped to $63,064 (**-58.7%**). Active stores declined to 180 (**-16.3%**) and maximum stock fell to 123,765 (**-73.7%**). The key counter-signal is price: average account price rose from $6.86 to $11.03 (**+60.8%**), suggesting that while fewer accounts were sold, the remaining supply skewed toward higher-value hotel, loyalty or booking accounts.

This decline is unlikely to reflect weaker travel demand alone. Q2 normally benefits from summer travel planning and Memorial Day demand; the American Automobile Association (AAA) projected record 2026 Memorial Day travel, with 45M Americans expected to travel at least 50 miles. Against a broadly stable seller population, the movement is concentrated: one marketplace more than doubled accommodation stock (from 2,262 to 5,148), while several higher-volume sellers pulled back.

74% ▼
Account Sales

59% ▲
Revenue

16% ▼
Active Shops

74% ▼
Total Stock

1
Malicious Configs

11
Brands Targeted

61% ▲
Average Price

THREAT: **GIFT CARD FRAUD**

868 Sales on criminal marketplaces	**23.6K** Stock on criminal marketplaces
$12.2K Revenue from criminal marketplaces sales	**$14.07** Average Price

TOP THREAT DRIVERS

- Commoditization of attack infrastructure (booking-fraud and scraping operators rent proxies and solvers like any other sector).
- Agentic commerce (travel booking is an early agentic-commerce use case, agents booking rooms with customer authority).
- FIFA World Cup (the bundled travel-and-ticket packages, flights and Airbnb sold with tickets, put accommodation in the event-fraud path)

AIRLINES

THREAT: **ACCOUNT TAKEOVER**

Observed airline sell-through fell to 10,994 sold (**-54.7%**), with revenue dropping to $60,620 (**-78.4%**). Average price declined from $11.54 to $5.54 (**-52.0%**), while active stores fell to 208 (**-13.3%**) and stock dropped to 123,070 (**-61.9%**). Airlines is the one industry where both volume and price compressed, pointing to lower value residual inventory rather than a shift upmarket.

The fall held despite summer and Memorial Day travel pressure, when airline portals see heavier legitimate logins. Movement concentrated in a few sellers against a stable population. One marketplace grew airline sell-through more than 17x, from 924 to 16,198, but that single surge could not offset pullbacks elsewhere. The result is a market that stayed active but thinner, cheaper and more fragmented than Q1.

55% ▼
Account Sales

78% ▼
Revenue

13% ▼
Active Shops

62% ▼
Total Stock

1
Malicious Configs

32
Brands Targeted

52% ▼
Average Price

THREAT: **GIFT CARD FRAUD**

2.2K Sales on criminal marketplaces	**2.1K** Stock on criminal marketplaces
$10.6K Revenue from criminal marketplaces sales	**$4.79** Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (loyalty-account credential stuffing benefits from AI-accelerated re-tooling).
- Agentic commerce (flight booking is a flagship agentic use case, high-consequence when an agent transacts with full authority).
- Commoditization of attack infrastructure (fare-scraping, loyalty-account ATO, and seat-bots run on rented capability)

ENTERTAINMENT & TICKETING

THREAT: **ACCOUNT TAKEOVER**

Entertainment and ticketing was one of the few categories where revenue grew despite lower volume. Sales fell to 8,558 (**-16.2%**), but revenue rose to $39,246 (**+22.4%**) and average price increased to $4.59 (**+46.2%**). Stores fell slightly to 268 (**-6.6%**), and stock declined to 443,096 (**-30.1%**).

Revenue growth on lower volume points to a lower-supply, higher-value market rather than weaker demand. Q2 coincided with heavy sports and live-event demand, including the 2026 FIFA World Cup ticket cycle which saw inflated prices due to glitch-affected ticket sales in April The top continuing sellers in this vertical all increased unit sales, some significantly, which supports the higher-value read against an otherwise stable storefront count.

16% ▼
Account Sales

22% ▲
Revenue

7% ▼
Active Shops

30% ▼
Total Stock

1
Malicious Configs

17
Brands Targeted

46% ▲
Average Price

THREAT: **GIFT CARD FRAUD**

4.2K Sales on criminal marketplaces	**5.5K** Stock on criminal marketplaces
$29.8K Revenue from criminal marketplaces sales	**$7.02** Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (queue-evasion and bypass tooling re-tooled with AI assistance).
- Commoditization of attack infrastructure (scalping runs on rented bots, proxies, and premade accounts).
- FIFA World Cup (the core sector, scalping, queue evasion, resale routing, ballot-entry account-gen all target ticketing).

FINANCE

THREAT: **ACCOUNT TAKEOVER**

Observed financial account sales fell from 102,444 to 69,648 (**-32.0%**) and revenue dropped more sharply from $181,656 to $71,000 (**-60.9%**). Maximum stock fell from 2.78M to 1.83M (**-34.1%**) and average price compressed from $1.77 to $1.02 (-**42.4%**), indicating that the remaining inventory was cheaper and likely lower-value than the accounts sold in Q1.

Finance is the structural exception to this quarter's stable population pattern: active stores declined from 63 to 35 (**-44.4%**). One reading is real contraction, with higher-value banking, fintech and balance-bearing accounts not replaced as sellers left. The other is displacement: financial fraud draws the most regulatory and enforcement pressure, pushing high-value sellers to invite-only forums and private deals. These accounts stay attractive for cashout, refund fraud, mule onboarding and identity enrichment, so Q2 may reflect reduced visibility as much as reduced trade.

32% ▼
Account Sales

61% ▼
Revenue

44% ▼
Active Shops

34 ▼
Total Stock

6
Malicious Configs

38
Brands Targeted

42% ▼
Average Price

TOP THREAT DRIVERS

- AI as a force multiplier ($900M in AI-related scam losses per the FBI report, synthetic-content fraud hits finance hardest).
- Agentic commerce (agents acting with financial authority; the CFAA/authorized-activity question is a finance-adjacent legal risk).
- Commoditization of attack infrastructure (ATO and credential stuffing against banking run on the rented frontier/services stack)

GAMING

THREAT: **ACCOUNT TAKEOVER**

Gaming saw the sharpest observed disruption in Q2. Sales collapsed from 15,759 to 1,324 (**-91.6%**), while revenue fell more moderately from $31,300 to $19,131 (**-38.9%**). Average price surged from $1.99 to $14.45 (**+626.1%**), despite stores only falling from 1,576 to 1,443 (**-8.4%**) and stock dropping from 2.52M to 1.33M (**-47.2%**). The price spike indicates scarcity: fewer accounts moved, but the accounts that remained available were priced as higher-value, harder-to-source inventory.

The collapse was primarily a seller-side shock. Four gaming-focused providers that went offline had sold 14,019 gaming units in Q1, almost the same scale as the category's total observed decline of 14,435. A fifth major provider sold 5,634 gaming units in Q1 but shifted focus in Q2 toward webmail/email logs, removing another major source of gaming inventory. This happened despite normal Q2 demand drivers, including Steam's official Summer Sale (June 25–July 9) and multiple Steam fests across April–June, so the decline is best read as major supply disappearing, not a loss of adversary interest in gaming accounts.

Configuration activity ran the other way: gaming drew the most malicious configurations of any industry at 12, so adversary tooling held up even as sell-through collapsed.

92% ▼
Account Sales

39% ▼
Revenue

8% ▼
Active Shops

47% ▼
Total Stock

12
Malicious Configs

16
Brands Targeted

626% ▲
Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (jailbroken-account market and AI-assisted bypass, directly relevant to anti-cheat and client protection).
- Commoditization of attack infrastructure (account farming, ATO, and in-game-asset fraud run on rented tooling and cheap accounts).

QUICK SERVICE RESTAURANTS (QSR)

THREAT: **ACCOUNT TAKEOVER**

Observed QSR account sales fell to 22,594 (**-62.7%**), with revenue down to $53,706 (**-52.9%**). Average price rose to $2.38 (**+26.6%**), while stores were broadly flat at 664 (**-1.2%**) and stock fell to 1.84M (**-42.2%**). The category remains active, but Q2 lost a large portion of the bulk supply seen in Q1.

The continuing-seller data shows mixed dynamics: the largest continuing seller declined modestly, while several others grew strongly, including one that more than tripled units. That means the drop is mainly a supply concentration problem rather than a collapse in QSR abuse demand. QSR accounts remain attractive because mobile ordering, loyalty balances, saved payment details and gift cards allow fast monetization. Kasada has previously highlighted QSR as a major ATO target as digital ordering expands the attack surface.

63% ▼
Account Sales

53% ▼
Revenue

1% ▼
Active Shops

42% ▼
Total Stock

0
Malicious Configs

77
Brands Targeted

27% ▲
Average Price

THREAT: **GIFT CARD FRAUD**

3.7K Sales on criminal marketplaces	**216.1K** Stock on criminal marketplaces
$50.4K Revenue from criminal marketplaces sales	**$13.65** Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (loyalty-account credential stuffing accelerated by AI re-tooling).
- Agentic commerce (agent-placed food orders are an emerging low-volume, high-authority surface).
- Commoditization of attack infrastructure (loyalty-points fraud, promo/coupon abuse, and account farming run on rented accounts and proxies).

RETAIL

THREAT: **ACCOUNT TAKEOVER**

Retail was the most stable industry. Observed retail account sales were effectively flat at 145,283 (**-0.02%**), while revenue rose sharply to $505,074 (**+39.7%**) and average price increased to $3.48 (**+39.8%**). Stores increased to 1,531 (**+5.2%**), even as stock halved to 2.73M (**-49.7%**).

The market appears to have shifted from bulk availability to higher-value retail accounts with better monetization potential, such as stored cards, loyalty balances, gift cards or premium eCommerce profiles. The top continuing sellers all grew, some by several hundred percent, which explains why retail avoided the deep volume collapse seen elsewhere. Late-Q2/early-Q3 shopping momentum also mattered: Prime Day 2026 activity began building into early July, with early deals already available by the tail end of June in some regions.

0%
Account Sales

40% ▲
Revenue

5% ▲
Active Shops

50% ▼
Total Stock

9
Malicious Configs

90
Brands Targeted

40% ▲
Average Price

THREAT: **GIFT CARD FRAUD**

3.7K Sales on criminal marketplaces	**32.6K** Stock on criminal marketplaces
$24.6K Revenue from criminal marketplaces sales	**$6.63** Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (checkout-bot bypass tooling re-tooled with AI).
- Agentic commerce (Google Shopping, Shopify, Anthropic agentic-commerce adoption is retail-first).
- Commoditization of attack infrastructure (the checkout-bot economy, 94% rent rather than build, is the retail story),
- FIFA World Cup (the retail-flip economy around merch, trading cards, LEGO, and licensed apparel treating the tournament as a retail event).

SOCIAL NETWORKS

THREAT: **ACCOUNT TAKEOVER**

Observed social network account sales fell from 63,890 to 2,239 (**-96.5%**), with revenue dropping from $41,636 to $3,445 (**-91.7%**). Stock almost halved from 1.81M to 920,672 (**-49.0%**), while store count was effectively flat (1,173 to 1,177). Average price rose from $0.65 to $1.54 (**+136.9%**), showing that the remaining market was thinner but more expensive.

Similar to the gaming vertical, the per-seller data explains the severity of the fall. Five social network account sellers that went offline had sold 39,786 units in Q1, accounting for roughly 65% of the total observed Q1-to-Q2 decline in the industry. The remainder is consistent with surviving sellers either reducing volume or shifting focus, leaving no replacement source to absorb demand. Social network accounts remain valuable for scams, impersonation, spam and malware distribution. The Q2 result reflects marketplace disruption and channel fragmentation, consistent with reporting on Telegram blocking and underground migration, rather than a fall in criminal demand.

97% ▼
Account Sales

92% ▼
Revenue

0%
Active Shops

49% ▼
Total Stock

1
Malicious Configs

20
Brands Targeted

137% ▲
Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (synthetic content, fake accounts, AI-generated social proof, and the $900M synthetic-content scam figure land here).
- Agentic commerce (agents acting on social platforms, and the phishing-agent research showing AI browsers turned into scam machines).
- Commoditization of attack infrastructure (bulk account creation and the account market feed fake-engagement operations).

STREAMING

THREAT: **ACCOUNT TAKEOVER**

Observed streaming account sales declined to 18,662 (**-24.3%**), but revenue increased to $180,846 (**+66.9%**) and average price rose from $4.39 to $9.69 (**+120.7%**). Stores increased to 2,091 (**+5.4%**), while stock fell to 1.49M (**-42.1%**).

This is a quality-over-quantity pattern against a growing storefront count. The leading continuing sellers remained active and several grew, while lower-value inventory thinned out. Streaming platforms' account-sharing enforcement continues to raise the value of accounts that remain stable: Netflix states that accounts may not be shared outside the household unless an extra member is added and HBO Max offers a paid extra-member add-on for out-of-household sharing. As cheap access becomes less durable, buyers appear willing to pay more for verified, longer-lived accounts.

24% ▼
Account Sales

67% ▲
Revenue

5% ▲
Active Shops

42% ▼
Total Stock

10
Malicious Configs

70
Brands Targeted

121% ▲
Average Price

THREAT: **GIFT CARD FRAUD**

3.7K Sales on criminal marketplaces	**5.9K** Stock on criminal marketplaces
$26.9K Revenue from criminal marketplaces sales	**$7.22** Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (credential-stuffing re-tooling against streaming ATO).
- Commoditization of attack infrastructure (IPTV panels, credential stuffing for account access, and proxy infrastructure are rented).
- FIFA World Cup (streaming piracy is a named World Cup threat, the 13 IPTV services, Operation Offsides, credential-theft delivery vector).

WEBMAIL

THREAT: **ACCOUNT TAKEOVER**

Observed webmail account sales dropped from 197,193 to 2,842 (**-98.6%**), with revenue falling from $85,237 to $3,830 (**-95.5%**). Stores actually increased slightly from 576 to 586 (**+1.7%**), but maximum stock fell from 2.17M to 889,432 (**-59.0%**). Average price rose from $0.43 to $1.35 (**+214.0%**), reflecting a market where bulk supply disappeared and remaining accounts became relatively scarce.

This was overwhelmingly driven by large providers going offline. Five webmail sellers that went offline in Q2 had collectively sold 244,614 webmail units in Q1, including 239,797 units from the three largest providers alone. This exceeded the total observed Q1-to-Q2 category decline of 194,351 units, confirming that the collapse was driven by the loss of major bulk suppliers rather than a reduction in the underlying value of webmail accounts. Webmail remains a core ATO enabler because compromised inboxes support password resets, phishing, and pivots into other services; infostealers and botnets continue to replenish those credentials even when individual marketplaces or sellers disappear.

99% ▼
Account Sales

96% ▼
Revenue

2% ▲
Active Shops

59% ▼
Total Stock

5
Malicious Configs

16
Brands Targeted

214% ▲
Average Price

TOP THREAT DRIVERS

- AI as a force multiplier (OpenBullet credential stuffing and AI-assisted bypass target webmail as the account layer).
- Commoditization of attack infrastructure (bulk email accounts are core inventory and underpin the whole account economy).
- FIFA World Cup (bulk mail as a stated input to the ballot-entry/account-gen fraud).

FULL PREDICTIONS & CURRENT STATUS

AI & Automation

AI-01 AI-native adversaries emerge

Partially

AI-native adversaries emerge: entire operations built around autonomous agents, not just AI-assisted human operators.

AI-02 AI v. AI arms race

Starting

AI v. AI arms race: adversaries using AI detect and respond to defensive changes far faster than was previously possible.

AI-03 Bot operators overcome AI scepticism

Partially

Bot operators overcome AI scepticism as reliability improves in H1 2026; AI becomes viewed as mission-critical infrastructure.

AI-04 Novices build working bots using AI

Starting

Complete novices build production-ready bots in under 60 minutes using AI assistance; technical barrier largely eliminated.

AI-05 AI automates raffle entry

Not Observed

AI automates raffles: widespread adoption of AI-powered raffle/drop entry systems across bot communities.

AI-06 Server-side AI monitoring

Starting

Server-side AI monitoring goes mainstream: 'AI detects inventory before it's live' technology widely adopted by bot operators.

AI-07 AI agents replace single massive traffic spikes

Starting

AI agents replace single massive traffic spikes with thousands of slow, legitimate-looking 'window shopper' sessions performing complex, resource-intensive searches.

AI-08 Gray area AI-driven shopping research

Starting

AI-driven shopping research at inhuman scale occupies an ambiguous regulatory/legal space; agents may not technically violate ToS.

AI-09 Block v. allow dilemma intensifies

Partially

Platform dilemma intensifies: blocking AI agents risks losing discoverability; allowing them risks mass unauthorised content scraping.

AI-10 Credential-to-cash conversion times drop

Partially

Legal precedents lag behind technology: court rulings based on older scraping techniques become obsolete as agentic AI introduces new methods.

Account takeover

ATO-01 AI-native adversaries emerge

Partially

'Fresh credential' marketplaces emerge, tiering stolen credentials by age, account value, and associated session data.

ATO-02 Credential packages expand

Occurring

Credential packages expand beyond passwords to include MFA tokens, session cookies, and device fingerprints.

ATO-03 AI-powered credential stuffing grows

Starting

Credential packages expand beyond passwords to include MFA tokens, session cookies, and device fingerprints.

ATO-04 Cross-platform credential correlation

Early signs

Cross-platform credential correlation enables adversaries to map victims' entire digital footprints from a single credential set.

ATO-05 Credential-to-cash conversion times drop

Starting

Credential-to-cash conversion times drop significantly due to automation and improved tooling.

Enablers

ENA-01 N/A - DUPLICATIVE

Retired - Q1

The most successful bot operations will be the ones retailers never hear about.

ENA-02 Barrier to bot ops is financial > technical

Starting

Barrier to entry for successful bot operations becomes predominantly financial rather than technical.

ENA-03 Gap widens between budget & funded ops

Starting

Gap widens between budget botters and well-funded operations; one-size-fits-all anti-bot services become ineffective against well-resourced adversaries.

ENA-04 Low forum mentions indicate bot success

Occurring

Lower forum mentions correlate with higher actual bot success rates: reduced public chatter signals effective operation.

ENA-05 Malicious ASNs prevail

Occurring

ASNs with 98%+ malicious traffic maintain relationships with major cloud/CDN providers despite awareness of adversarial use.

ENA-06 IP reputation collapses

Occurring

IP reputation collapses as clean residential proxies become commodity infrastructure accessible at low cost.

Reselling

RES-01 AI-generated 'social proof' expands

Partially

AI-generated 'social proof' expands beyond fake reviews to include fake unboxing videos, AI influencer endorsements, and synthetic social media accounts.

RES-02 'Flash scalping' operations emerge

Early signs

'Flash scalping' operations emerge: AI identifies, targets, and depletes inventory within minutes of products gaining social media traction.

RES-03 TikTok Shop as major fraud surface

Partially

TikTok Shop becomes a major fraud battleground: $87B in projected 2026 sales creates massive new attack surfaces via thousands of seller integrations.

RES-04 Social capital as a key driver for reselling

Partially

Reselling remains heavily influenced by social capital: virality and 'meme level' remain the primary demand signals for targeted botting.

RES-05 Scalpers employ more sophisticated bots

Starting

Scalpers employ more sophisticated automation (next-gen bots) focused on account distribution, identity masking, and rapid off-platform transactions.

RES-06 Regulatory crackdowns push underground

Early signs

Regulatory crackdowns push transactions underground: encrypted P2P marketplaces and private Discord/Telegram channels grow.

RES-07 Scalpers shift focus to less regulated Items

Occurring

Problem displacement: professional scalpers shift focus to goods with weaker regulations (sneakers, collectibles, gaming consoles).

RES-08 N/A - DUPLICATIVE

Retired - Q2

Rise of encrypted channels makes enforcement significantly harder and measurement of the problem increasingly difficult.

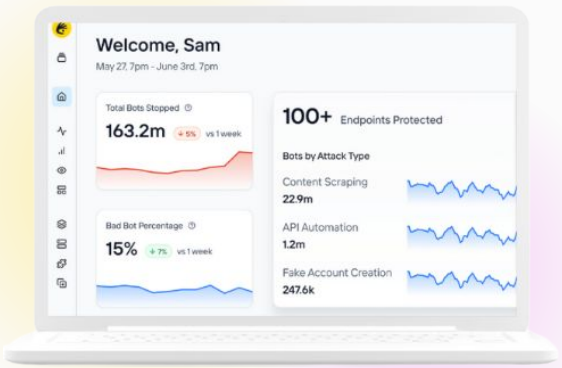
Looking Ahead

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 behavior 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.

About Kasada

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

kasada

For more information,
please visit our website.

kasada.io →

Email us: team-threat-intel@kasada.io

Connect with KasadaIQ on: