# RETAIL INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS

## RETAIL INDUSTRY ATTACK POINTS

The retail sector experienced broad growth in attack frequency but a decline in overall traffic, suggesting an increase in smaller, lower-impact activity. One possible interpretation is that promotional or referral abuse contributed to higher counts of lightweight sign-up events.

**Focus on Sign-Up: Increased Frequency, Reduced Traffic**

| | | |
|---|---|---|
| Attacks: +97% | Malicious traffic: -55% | Average attack size: -77% |

Sign-up activity nearly doubled in frequency but generated significantly less traffic per event, diverging sharply from the industry-wide sign-up malicious traffic change (+27%).

What This Reveals

The data shows that the retail industry's Q2 sign-up activity became more diffuse, with more frequent but lower-volume events. These patterns align with promotional or account creation abuse that relies on high repetition rather than intensive throughput.

## RETAIL INDUSTRY ATTACK TYPES

Retail platforms continued to face consistent pressure from fake account creation in Q2 2025. Fraudsters are likely attempting to exploit sign-up promotions and rewards programs that provide immediate value upon registration.

**Fake Account Creation: Nearly Doubled Quarter Over Quarter**

| | | |
|---|---|---|
| Attacks: +97% | Malicious traffic: -55% | Average attack size: -77% |

Attack frequency nearly doubled in Q2, while total malicious traffic dropped by more than half. The divergence between count and traffic suggests a rise in smaller, faster automated sign-up attempts—optimized for speed and volume rather than sustained throughput.

What This Reveals

Retail's Q2 data reinforces how registration abuse remains a dominant attack type for the sector. Fraudsters are prioritizing lightweight automation to exploit welcome bonuses, referral credits and loyalty incentives. The shrinking attack size indicates a shift toward higher efficiency rather than brute-force scale.

# RETAIL INDUSTRY ATTACK MECHANISMS

Retail platforms experienced substantial growth in attack volume during Q2 2025, with both bots and automation services expanding but showing divergent traffic patterns.

**Attack Distribution**

- **Bots:** 65% of attacks (up from 45% in Q1)
- **Attack automation services:** 35% of attacks (down from 55% in Q1)

**Quarter-Over-Quarter Changes**

- **Attack automation services:** +28% attacks, -58% malicious traffic, -67% average attack size
- **Bots:** +180% attacks, -52% malicious traffic, -83% average attack size

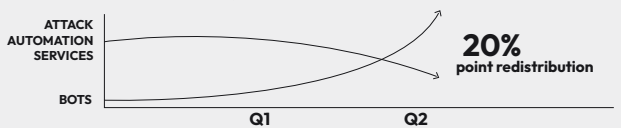
What This Reveals

Retail platforms saw a dramatic reversal in mechanism distribution, with bots surging from 45% to 65% of attacks—a 20-percentage-point swing that mirrors patterns observed in gig economy platforms. Both bots and automation services grew substantially in frequency while generating significantly less malicious traffic,indicating a fundamental shift toward smaller, more distributed attacks.

The large decline in average bot attack size represents the most extreme fragmentation observed across any industry, suggesting attackers shifted from sustained volumetric campaigns to rapid, lightweight probing. Attack automation service attacks similarly became smaller on average despite growing in frequency, diverging from the cross-industry pattern where attack automation service traffic grew.

While attack automation services declined significantly as a proportion of total attacks, the growth in absolute volume—combined with retail's rapid adoption of mobile commerce infrastructure—suggests this category warrants close monitoring in future quarters.

**Q1→ Q2 MECHANISM SHARE SHIFT**



# RETAIL INDUSTRY ATTACK BROWSERS & DEVICES

**Chrome Dominance with Limited Browser Diversity**

Chrome captured the majority of all retail attacks in Q2, maintaining its position as the overwhelmingly preferred attack browser. Unlike other industries with extensive browser diversity in their top rankings, retail showed remarkable simplification with only a handful of browsers appearing alongside Chrome, Chrome Mobile, Headless Chrome and Chrome Webview. This extreme consolidation suggests retail attackers are abandoning specialized or niche browsers (Python Requests, Roblox, Vivaldi, WeChat) that appeared in Q1 but essentially disappeared by Q2.

**Dramatic Device Shift Toward Mobile**

Retail platforms experienced one of the most significant device distribution changes across all industries analyzed.

- **Attacks via desktop:** Grew 35%
- **Attacks via mobile:** Surged 180%
- **Device distribution:** Shifted from 70% desktop/30% mobile to 53%desktop/47% mobile

**Key Takeaways**

The disproportionate decline in mobile attacks, combined with Mobile Safari's collapse and the disappearance of mobile-specific browsers like Android Browser, suggests attackers are consolidating their efforts on desktop-based tools. This may reflect better automation capabilities on desktop platforms, defensive improvements on mobile channels, or changes in authentication methods that favor desktop-based automation.

**TOP BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP AND MOBILE DEVICES – RETAIL INDUSTRY, Q2 2025**

| No. | Desktop (Q2) |
|---|---|
| 01 | Chrome |
| 02 | Headless Chrome |

| No. | Mobile (Q2) |
|---|---|
| 01 | Chrome Mobile |
| 02 | Mobile Safari |

## RETAIL INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that retail platforms face concentrated attack patterns from specific geographic regions. The top five attack origins alongside the United States—India, Great Britain, Mexico, Brazil and Vietnam—reflect distinct advantages for fraudsters targeting retail operations.

**Key Geographic Insights**

**Technological Infrastructure and Scale:** India has emerged as a major hub for cybercrime operations, with a robust digital infrastructure. The country's large IT workforce and relatively low operating costs enable fraudsters to run sophisticated operations at scale.

**Cross-Border Advantages:** Mexico's location provides unique advantages for retail fraud. The proximity to the U.S. market, combined with less stringent enforcement and the presence of organized cybercrime groups targeting financial accounts, creates an environment conducive to retail fraud operations.

**Regional Operations Centers:** The United States and Brazil serve as major hubs for both legitimate e-commerce and fraud operations. Their large domestic markets, advanced payment infrastructure and significant Portuguese and Spanish-speaking populations enable fraudsters to target multiple markets across the Americas while blending with legitimate traffic patterns.

**Southeast Asian Fraud Networks:** Vietnam's prominence in retail attack origins reflects the region's growing sophistication in e-commerce fraud. The country's combination of technical capabilities, organized fraud networks and strategic timezone positioning for targeting both Asian and Western markets makes it an increasingly important hub for retail-focused cybercrime operations.

| Retail Industry: Top 6 Attack Origins | |
|---|---|
|  | United States |
|  | India |
|  | Great Britain |
|  | Mexico |
|  | Brazil |
|  | Vietnam |

# RETAIL INDUSTRY RECOMMENDED ACTIONS

**Secure Mobile Commerce**

Implement advanced mobile device fingerprinting and app-mimicking detection. The transformation from desktop-dominated to mobile-majority attacks represents one of the most dramatic device shifts observed, indicating fraudsters are rapidly expanding mobile attack infrastructure for retail targets.

**Combat Promotional Abuse**

Deploy velocity controls, email verification and enhanced fraud scoring specifically during promotional periods. Smaller, faster automated sign-up attempts suggest fraudsters are optimizing for promotional exploitation rather than sustained account compromise campaigns.

**Adapt to Bot Resurgence**

Maintain adaptive bot detection that scales with attack intensity. The dramatic swing from automation services back to bots, mirroring gig economy patterns, suggests fraudsters are consolidating toward proven basic tools after sophisticated services faced defensive pressure.

**Monitor Browser Simplification**

Focus detection on mainstream browser anomalies. Retail experienced substantial browser consolidation, with diverse Q1 attack browsers vanishing by Q2, suggesting fraudsters have standardized their toolsets around Chrome and mobile browsers for the time being.

**Counter Regional Operations**

Apply risk-based authentication considering regional attack patterns and transaction characteristics. Keep in mind that India leads non-U.S. attacks with sophisticated IT infrastructure and scale capabilities, followed by Great Britain and Mexico.

## CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When retail platforms implement adaptive security and deploy detection systems tuned for evolving attack patterns, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, retail teams can move from reactive security to proactive defense—protecting not just transactions and customer data, but the shopping experiences that build brand loyalty.

## ABOUT ARKOSE LABS

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Trusted by the world's leading consumer brands—including two of the top three banks, Microsoft, Meta, Roblox, and many others—Arkose Labs stops account takeovers, fake account creation, LLM-driven scraping and SMS toll fraud. The platform actively undermines attacker ROI by introducing dynamic friction, making it economically unsustainable for adversaries to persist. Its Security Operations Center (SOC) provides actionable insights from an extensive cross-industry intelligence network, which monitors legitimate traffic and attack patterns across global enterprises. With unparalleled proactive support for internal security teams, Arkose Labs goes beyond conventional security by actively partnering with customers to disrupt organized fraud networks such as Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.

**USA** (San Mateo)

**Australia** (Brisbane)

**United Kingdom** (London)

**Costa Rica** (San José)

**India** (Pune)

**Argentina** (Buenos Aires)

Book a Meeting