GAMING INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS™

GAMING INDUSTRY ATTACK POINTS

The gaming industry's attack patterns reveal a complex ecosystem. While sign-up remains a dominant attack point, virtual economies attract increasingly sophisticated fraud operations—with shifts in both attack intensity and targeting strategies.

Payment Attacks: Concentrated Growth

Attacks: +54%	Malicious traffic: +866%	Average attack size: +528%

Payment-related malicious traffic increased at the highest rate observed across any gaming attack point. The disparity between traffic and attack volume indicates larger-scale, higher-throughput activity against payment channels.

Account Management: Increased Frequency, Smaller Scale

Attacks: +80%	Malicious traffic: +33%	Average attack size: −26%

Account management attacks rose sharply in number but produced smaller average traffic volumes per event. The increase in frequency suggests sustained, lower-intensity activity within user profile or inventory functions.

Sign-In: Moderate Decline

Attacks: -8%	Malicious traffic: -26%	Average attack size: -20%

Sign-in activity declined in both volume and traffic, reducing its share of overall gaming-related activity compared with the previous quarter.

What This Reveals

Gaming's attack landscape demonstrates a monetization pivot. The payment point malicious traffic surge, combined with the rise in account management attacks indicates fraudsters are moving beyond simple account theft to focus on extracting value from compromised accounts.

GAMING INDUSTRY ATTACK TYPES

The gaming industry experienced broad but uneven movement in Q2 2025, with clear surges in payment-related attacks and continued volatility in credential-based activity. One likely driver: Expanding in-game economies and payment integrations have made transactional endpoints especially lucrative for attackers seeking quick monetization.

Payment-Based Attacks: Surge in Transactional Abuse

Attacks: +54%	Malicious traffic: +866%	Average attack size: +528%

Payment-based attacks rose more than any other gaming category. Traffic increased more than 9x, far exceeding overall industry baselines, indicating high-intensity targeting of in-game purchases, virtual currency and payment verification systems.

In-App Threats: Increased Frequency, Smaller Payloads

Attacks: +80%	Malicious traffic: +33%	Average attack size: –26%

In-app threats expanded significantly by volume, though the average attack size declined. The increase in frequency reflects sustained targeting of profile, inventory and rewards-management actions.

Account Takeover (ATO): Continued Contraction

Attacks: -5%	Malicious traffic: -26%	Average attack size: -22%

ATO activity declined across all measures, maintaining its role as a major but receding component of the gaming threat mix.

Fake Account Creation: Downward Adjustment in New-Account Abuse

Attacks: -16%	Malicious traffic: -33%	Average attack size: -20%

Registration abuse dropped quarter over quarter, mirroring improved friction at onboarding flows or attacker reprioritization toward post-authentication vectors.

What This Reveals

Gaming's Q2 distribution highlights an ongoing shift from credential-based compromise to transactional exploitation. Payment-based and in-app attacks combined to drive most of the observed activity, reinforcing the commercial incentive behind fraud targeting in-game value and monetization endpoints.

GAMING INDUSTRY ATTACK MECHANISMS

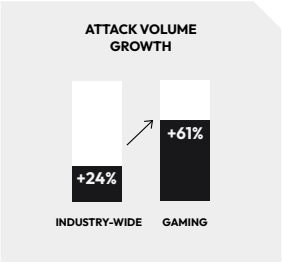
Gaming platforms saw sophisticated attack automation services gain significant ground, capturing share from traditional bot attacks.

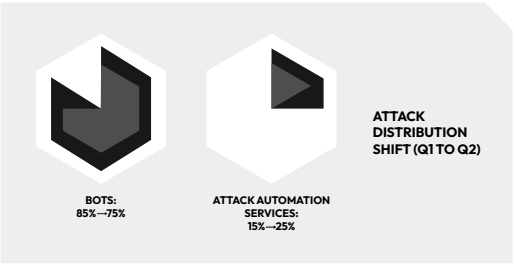
Automation Services Gain Ground

Attack automation services surged 61% in volume—2.5x higher than the industry-wide 24% increase. These services grew from 15% to 25% of all gaming attacks, indicating fraudsters are investing in professional automation platforms alongside traditional bot operations. Meanwhile, bot attacks fell 11% in volume with 24% less malicious traffic.

Attack Distribution Shift (Q1 to Q2):

- **Bots:** 85% → 75%
- **Attack automation services:** 15% → 25%
- **Human-assisted:** <1% (negligible volume)





What This Reveals

Gaming's mechanism shift shows an evolving fraud ecosystem where both basic bots and professional automation services coexist. The 10 percentage point share transfer from bots to automation services suggests fraudsters are expanding their toolsets, signaling increased investment in gaming fraud operations.

GAMING INDUSTRY ATTACK BROWSERS & DEVICES

Platform-Specific Attack Vectors

Roblox captures 18% of all gaming attacks—a platform-specific browser absent from other industries. This highlights attacks originating from within gaming environments themselves, where fraudsters exploit embedded browsers to blend with legitimate player traffic. Battle.net and Steam In-Game Overlay represent additional gaming-only entry points, indicating fraudsters are adapting their tools to each platform's unique architecture rather than relying solely on traditional web browsers.

Browser Consolidation and Geographic Indicators

Chrome variants (Chrome, Chrome Mobile, Chrome Mobile iOS) combine for over 46% of attacks. The presence of Yandex Browser (nearly 2%) suggests Eastern European fraud operations targeting gaming platforms.

Device Distribution Remains Stable

- **Attacks via desktop:** Grew slightly by nearly 1%
- **Attacks via mobile:** Declined by just over 4%
- **Device distribution:** 69% desktop/31% mobile to 70% desktop/30% mobile

Key Takeaways

Unlike industries showing dramatic device shifts, gaming's stable distribution suggests consistent attack methodologies across quarters with no significant changes in platform targeting strategies. The minimal variation indicates gaming platforms face steady attack patterns without the dramatic pivots seen in sectors like dating or fintech, potentially representing an equilibrium in attacker device preferences.

TOP 5 BROWSERS BY NUMBER OF ATTACKS, GAMING, Q2 2025

No.	Desktop Browsers
01	Chrome
02	Microsoft Edge
03	Opera
04	Firefox
05	Yandex Browser

No.	Mobile Browsers
01	Roblox
02	Chrome Mobile
03	Mobile Safari
04	Chrome
05	Chrome Mobile iOS

GAMING INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that traffic appearing to originate from the United States represents more than one-quarter of total attacks. This figure likely reflects widespread location masking by international threat actors attempting to appear legitimate. For this reason, we treat U.S. traffic as unknown when analyzing the data, and rank the countries with the highest apparent attack volumes besides the U.S. For the gaming industry, these countries are Great Britain (13%), Vietnam (9%) and Brazil (8%).

Key Geographic Insights

European Gaming Hub: Attacks appearing to originate from Great Britain and Germany emerge as major European sources, each contributing significant volumes. France adds another 3%, while smaller volumes appear to come from various European nations including Belgium, Poland and the Netherlands.

Latin American Operations: Brazil stands out with a consistent 7-8% share of apparent attacks across Q1 and Q2. Mexico contributes another nearly 1%, with other Latin American countries showing minimal presence.

Southeast Asian Concentration: Vietnam shows notable growth in apparent attack traffic to nearly 9%. The Philippines doubles from nearly 7% in Q2. Thailand remains stable at approximately 2% of attacks.

East Asian Presence: Hong Kong (just over 2%) and Japan (nearly 1%), along with mainland China and South Korea, show moderate but consistent apparent attack volumes.

Gaming Industry: Top 10 Attack Origins (Excluding U.S.)

	Great Britain
	Vietnam
	Brazil
	Philippines
	Germany
	France
	Indonesia
	Canada
	Hong Kong
	Thailand

Note: Data excludes U.S. traffic to account for attackers masking their true location.

GAMING INDUSTRY RECOMMENDED ACTIONS

Secure Payment Endpoints

Implement transaction monitoring, velocity limits on virtual currency purchases and behavioral analysis to detect unusual spending patterns that signal compromised accounts. Focus defensive resources on payment endpoints where fraudsters are concentrating their most intensive campaigns.

Monitor In-Game Economies

Deploy real-time monitoring of item transfers, trades and marketplace activity. Flag sudden changes in player behavior that indicate account compromise or item farming operations. Consider automated alerts for suspicious transaction patterns in virtual goods.

Combat Automation Services

Deploy adaptive challenges that scale with suspicious behavior and implement proof-of-work systems for high-value transactions. As fraudsters shift toward professional automation platforms, detection must evolve to catch sophisticated tooling rather than just basic bots.

Validate Mobile Traffic

Implement device fingerprinting to distinguish legitimate mobile players from emulators and device farms. With gaming-specific browsers like Roblox appearing in attack data, monitor for patterns that suggest attacks originating from within gaming environments themselves.

Geographic Risk Analysis

Apply enhanced verification for account changes originating from high-risk regions, particularly when combined with unusual gameplay patterns. Great Britain, Vietnam and Brazil show the highest concentration of non-U.S. attack traffic.

CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When gaming platforms implement transaction monitoring for payment-based attacks and deploy adaptive challenges that counter the shift toward attack automation services, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, gaming teams can move from reactive security to proactive defense—protecting not just accounts and in-game assets, but the player experience that makes gaming communities thrive.

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