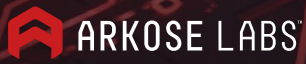
GIG INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025



GIG ECONOMY INDUSTRY ATTACK POINTS

The gig economy showed a mixed pattern in Q2 2025, with the most substantial growth concentrated in account management activity. This may suggest a continued focus on post-authentication exploitation, such as changes to payout details or identity information, which offer more direct opportunities for financial gain.

Account Management: Significant Growth in Traffic

Attacks: +5%	Malicious traffic: +411%	Average attack size: +388%

Account management activity recorded a sharp increase in malicious traffic, while the number of attacks grew only slightly.

Sign-In: Higher Frequency, Lower Volume

Attacks: +75%	Malicious traffic: -98%	Average attack size: -99%

Sign-in activity increased in count but saw a major reduction in overall traffic, indicating a higher number of smaller, less intensive events.

What This Reveals

The Q2 data shows a concentration of activity in account-management flows and a decline in attack volume across sign-in endpoints. This redistribution highlights a growing emphasis on modifying existing accounts rather than creating new ones.

GIG ECONOMY INDUSTRY ATTACK TYPES

The gig economy experienced uneven attack patterns in Q2 2025, characterized by a sharp rise in multifactor authentication (MFA) compromise alongside steep declines in fake account creation and SMS toll fraud. This distribution suggests attackers may be shifting tactics away from volume-based schemes toward more targeted verification abuse.

MFA Compromise: Rapid Escalation in Verification Abuse

Attacks: +5%	Malicious traffic: +411%	Average attack size: +388%

Although attack frequency rose only slightly, malicious traffic increased more than fivefold. This jump suggests higher-intensity targeting of authentication verification endpoints.

Account Takeover (ATO): Increased Attacks, Decreased Traffic

Attacks: +88%	Malicious traffic: -97%	Average attack size: -99%

While attacks nearly doubled, total traffic collapsed. The drastic decline in traffic and size indicates smaller, fragmented takeover attempts rather than broad credential campaigns.

Fake Account Creation: Decline in Activity

Attacks: -50%	Malicious traffic: -71%	Average attack size: -42%

Account-creation abuse declined sharply, reflecting reduced emphasis on large-scale registration activity within the gig ecosystem.

SMS Toll Fraud: Reduced Throughput

Attacks: -39%	Malicious traffic: -47%	Average attack size: -14%

Messaging-related fraud decreased across all metrics, falling below its prior dominant share of gig-related malicious traffic.

What This Reveals

The gig economy's threat profile shifted notably in Q2, with attackers concentrating resources on high-intensity MFA compromise while scaling back other schemes. The combination of elevated verification targeting and reduced SMS activity reflects an evolution in attack methodology, with fraudsters prioritizing sophisticated authentication bypass over mass account creation and SMS toll fraud.

GIG ECONOMY INDUSTRY ATTACK MECHANISMS

Attack automation service usage declined during Q2, dropping by more than half while the cross-industry growth was nearly 24%. This exodus from sophisticated tooling coincided with a 25 percentage point swing toward bots.

Attack Distribution (Q2)

- **Bots:** 66% of attacks (up from 40% in Q1)
- **Attack automation services:** 33% of attacks (down from 54% in Q1)
- **Human fraud farms:** 1% of attacks (down from 6% in Q1)

Quarter-over-Quarter Changes

- **Attack automation services:** -54% attacks, +9% malicious traffic, +136% average attack size
- **Bots:** +23% attacks, -35% malicious traffic, -47% average attack size
- **Human fraud farms:** -87% attacks, -93% malicious traffic, -48% average attack size

What This Reveals

The data reveals a paradox: automation service attacks became 136% larger on average despite declining 54% in frequency, while bot attacks grew in number but generated 35% less malicious traffic. This indicates a shift toward lightweight, high-frequency probing.

Most notably, human fraud farm activity essentially vanished, collapsing in frequency and in traffic—while the cross-industry growth was nearly +13%. The gig economy was one of few sectors to experience overall contraction, with total attacks declining 25%, compared to cross-industry volume that grew +7%.

GIG ECONOMY INDUSTRY ATTACK BROWSERS & DEVICES

Chrome Ecosystem Concentration

Chrome's dominance intensified to more than half of all attacks, while Chrome variants collectively represent the majority of browser signatures. Chrome Webview maintains its position as the second most common browser—which could indicate in-app activity, browser spoofing or automated tools.

Dramatic Browser Consolidation

Mobile Safari's share dropped by more than half (from 13% to 5%), while Firefox also declined notably. Multiple Q1 browsers—including Roblox, Android Browser, Python Requests and LinkedIn—all but disappeared by Q2. Internet Explorer appears in the top 10 despite being discontinued, while Whale Browser also makes the list.

Device Distribution Shifts Toward Desktop

While overall attacks declined 25%, the device distribution underwent notable change, contrasting with the industry-wide pattern of relative stability. Device distribution: Shifted from 67% desktop/33% mobile to 72% desktop/28% 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 gig platform authentication methods that favor desktop-based automation.

TOP 5 BROWSERS BY NUMBER OF ATTACKS, GIG ECONOMY, Q2 2025

No.	Desktop Browsers
01	Chrome
02	Firefox
03	Microsoft Edge
04	Chrome Mobile
05	Internet Explorer

No.	Mobile Browsers
01	Chrome Webview
02	Mobile Safari
03	Chrome Mobile
04	Chrome
05	Microsoft Edge

GIG ECONOMY INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that traffic appearing to originate from the United States represents 44% of total gig economy 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 gig economy companies, these are Brazil and Great Britain (nearly 8% each), followed by Canada (nearly 4%).

Key Geographic Insights

South American Operations: Brazil leads non-U.S. attack traffic at nearly 8%, with Peru contributing another almost 2%. Other South American countries show minimal presence in the attack data.

European Distribution: Great Britain matches Brazil at 8% of apparent attacks, while Germany contributes roughly 3%. Smaller volumes appear from Italy, France and various other European nations.

Asian Fraud Clusters: South Korea shows notable activity at almost 3%, with India, Vietnam and other Asian nations contributing smaller volumes. This is a relatively lower Asian presence compared to other industries.

Commonwealth Presence: Canada (4%) and Australia (2%) show consistent apparent attack volumes.

Emerging Markets: Countries like Bangladesh, Bolivia and various African nations show small but steady presence.

Gig Economy: Top 10 Attack Origins (Excluding U.S.)
Brazil
Great Britain
Canada
South Korea
Germany
Australia
India
Peru
Russia
Tajikistan

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

GIG ECONOMY INDUSTRY RECOMMENDED ACTIONS

Fortify Account Management

Deploy continuous authentication and anomaly detection to catch payout detail changes, identity modifications and unauthorized account access. Monitor for patterns indicating fraudsters are targeting post-authentication flows where they can directly modify worker payment information.

Counter MFA Compromise

Implement phishing-resistant authentication methods and educate users about session hijacking attempts. As fraudsters launch highly targeted campaigns against verification systems, traditional MFA alone may not provide sufficient protection.

Monitor Desktop Consolidation

Enhance desktop browser fingerprinting and behavioral analysis. The shift toward desktop infrastructure suggests sophisticated desktop-based tools are now targeting gig platforms more effectively than mobile attack vectors.

Address Bot Resurgence

Maintain robust bot detection while monitoring for automation service evolution. The dramatic swing back toward bots suggests defensive pressure pushed fraudsters away from automated service tools—but they may return with improved capabilities.

Geographic Intelligence

Deploy enhanced verification for high-risk regions, particularly for payout changes or identity modifications. Pay close attention to traffic emanating from Brazil, Great Britain and Canada, as they are the leading non-U.S. attack sources.

CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When gig economy platforms implement continuous authentication for account management functions and deploy phishing-resistant methods to counter MFA compromise, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, gig economy teams can move from reactive security to proactive defense—protecting not just worker accounts and payment information, but the economic opportunities that define the gig economy.

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