OTA INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS

OTA INDUSTRY ATTACK POINTS

Online travel agencies showed divergent trends in Q2 2025. Account management activity increased in frequency, while sign-in malicious traffic grew significantly despite fewer overall attacks. This distribution may indicate parallel testing of smaller-scale account modifications and larger authentication-based attempts.

Account Management: More Frequent, Smaller Events

Attacks: +161%	Malicious traffic: −46%	Average attack size: −79%

The number of attacks against account management flows increased notably, but average event size decreased, producing a decline in total malicious traffic.

Sign-In: Fewer Events, Heavier Traffic

Attacks: −33%	Malicious traffic: +344%	Average attack size: +566%

Although attack volume fell, total traffic grew considerably, resulting in much larger events on average.

What This Reveals

The OTA sector exhibited two distinct patterns—smaller, more frequent account management activity and larger, less frequent sign-in attempts. Together, these trends suggest shifting emphasis between persistence and intensity across separate attack vectors.

OTA INDUSTRY ATTACK TYPES

In Q2 2025, OTAs observed sharp growth in in-app threats and a reduction in account takeover (ATO) events. One likely explanation? Attackers appear to be splitting their focus between large-scale account modification campaigns and smaller, higher-value takeover attempts.

In-App Threats: Sustained Growth in Account Modification Activity

Attacks: +161%

In-app threats more than doubled quarter over quarter, marking a major rise in post-authentication manipulation. The increase suggests concentrated targeting of booking, loyalty and stored payment features tied to authenticated sessions.

Account Takeover (ATO): Fewer Incidents, Heavier Activity per Event

Attacks: −33%

ATO attack counts declined, yet underlying activity per campaign intensified, with higher traffic and average size per event. The trend points to more selective, resource-heavy takeover attempts against specific high-value user accounts.

What This Reveals

The Q2 data underscores a dual threat for OTAs: the steady escalation of authenticated account manipulation and the persistence of targeted, high-impact takeover efforts. Together, these two attack vectors continue to define the OTA threat landscape.

OTA INDUSTRY ATTACK MECHANISMS

Online travel agencies experienced bots surging to dominance while automation services contracted sharply in Q2 2025.

Attack Distribution*

- **Bots:** 70% of attacks (up from 66% in Q1)
- **Attack automation services:** 26% of attacks (down from 32% in Q1)
- **Human fraud farms:** 3% of attacks (up from 2% in Q1)

Quarter-Over-Quarter Changes

- **Attack automation services:** +77% attacks, -61% malicious traffic, -78% average attack size
- **Bots:** +126% attacks, -19% malicious traffic, -64% average attack size
- **Human fraud farms:** +200% attacks, +3,244% malicious traffic, +1,015% average attack size**

*Note, percentages do not add to 100% because of rounding.

**Human fraud farm percentages reflect growth from an extremely small baseline, making percentage changes less meaningful.

What This Reveals

OTA platforms saw bot attacks more than double while generating less total malicious traffic—the opposite of the cross-industry pattern where bot traffic grew +22% despite flat attack volume. The decline in average bot attack size represents the one of the steepest reductions across any industry analyzed, suggesting a shift toward high-frequency probing rather than sustained campaigns.

Automation service attacks grew in frequency but experienced a drop in malicious traffic—diverging sharply from the cross-industry pattern. The reduction in average attack automation service attack size indicates attackers shifted from intensive campaigns to lightweight testing against OTA defenses.

Attack Automation Services: Average Attack Size

OTA INDUSTRY ATTACK BROWSERS & DEVICES

OTA platforms experienced the most extreme consolidation observed across all industries, with attacks concentrating heavily on desktop Chrome.

Unprecedented Chrome Dominance and Browser Simplification

Chrome captured 67% of all OTA attacks in Q2, up from 56% in Q1—the highest single-browser concentration across all industries analyzed. The attack landscape simplified dramatically, with only a handful of distinct browsers appearing in Q2 compared to 20+ in industries like gaming or fintech. Microsoft Edge rose in the rankings, while gaming-related browsers (such as Roblox) all but disappeared.

Extreme Desktop Consolidation

OTA platforms experienced the most dramatic device shift among all industries:

- **Device distribution:** Shifted from 65% desktop/35% mobile to 90% desktop/10% mobile
- **Desktop attacks:** Surged 185%
- **Mobile attacks:** Declined 43%

This 25 percentage point swing toward desktop far exceeds the stable 68% desktop/32% mobile industry-wide baseline, with mobile attacks essentially collapsing to low levels.

Key Takeaway

The combination of Chrome dominance, lowest browser diversity and desktop concentration suggests OTA attackers—at least for the moment—have standardized on a highly specific attack profile. Desktop tools appear to offer decisive advantages for OTA-specific attacks, or enhanced mobile security measures successfully force attackers to abandon mobile vectors.

TOP 3 BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP– OTA INDUSTRY, Q2 2025

No.	Desktop Browsers
01	Chrome
02	Microsoft Edge
03	Firefox

In the mobile attack landscape, only Chrome Webview and Mobile Safari showed any measurable activity—all other mobile browsers recorded negligible attacks.

OTA INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that traffic appearing to originate from the United States represents 31% of total OTA 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 OTAs, these countries are Hong Kong, Mexico, China and Great Britain.

Key Geographic Insights

East Asian Concentration: Hong Kong and Japan each lead non-U.S. attack traffic at 9%, with China and Singapore each contributing nearly 5%. Taiwan adds 2%—for a significant East Asian presence.

European Distribution: Great Britain apparently contributes nearly 5% of attacks, with Germany, Ukraine and Kyrgyzstan each with less than half that attack volume. Even smaller volumes appear from Finland, Romania and Slovenia, suggesting more dispersed European activity compared to other industries.

Emerging Markets: The presence of countries like Australia, Brazil, Cambodia, Malaysia, Myanmar, Namibia, Pakistan and Tonga, all hovering near 1%, indicates fraudsters may be operating from diverse, less-monitored locations.

OTA Industry: Top 5 Attack Origins (Excluding U.S.)

	Hong Kong
	Japan
	Mexico
	China
	Great Britain

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

OTA INDUSTRY RECOMMENDED ACTIONS

Protect Booking Transactions

Deploy adaptive MFA and transaction monitoring for booking modifications. The concentration of massively larger attacks on authentication endpoints suggests fraudsters are launching targeted campaigns against high-value travel accounts rather than opportunistic scanning.

Monitor Desktop Consolidation

Enhance desktop behavioral analysis. OTAs experienced the most extreme device shift among all industries, with desktop attacks surging while mobile attacks declined dramatically, suggesting desktop tools offer superior capabilities for OTA-specific attacks.

Leverage Chrome Intelligence

Focus detection efforts on Chrome-specific fingerprinting anomalies. Chrome's extreme concentration—the highest single-browser dominance across all Industries—combined with simplified browser diversity indicates fraudsters have standardized their attack toolsets.

Address Attack Fragmentation

Deploy detection systems tuned for distributed, rapid-fire attempts rather than sustained campaigns. Both bots and automation services shifted toward lightweight, high-frequency probing rather than intensive attacks.

Geographic Risk Profiling

Apply enhanced verification for booking modifications from high-risk regions, particularly for last-minute changes. Pay close attention to traffic emanating from Hong Kong, Japan and Mexico, as each are notable originations of attacks.

CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When online travel agency platforms implement adaptive authentication and deploy detection systems tuned for the unique attack patterns targeting booking and loyalty systems, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, OTA teams can move from reactive security to proactive defense—protecting not just bookings and loyalty points, but the travel experiences that connect people to the world.

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