Enterprises Under Attack: Quarterly Threat Actor Patterns

Industry Trends, Analysis and Benchmarks | Released Q3 2025

ARKOSE LABS

TABLE OF CONTENTS

INTRODUCTION

The threat landscape continues to fundamentally and rapidly shift, largely fueled by AI and crime-as-a-service (CaaS) platforms that act as accelerants for attacks. As this report reveals, Q2 2025 saw malicious traffic surge nearly 20% over Q1, with attack sizes growing more than 12%. But raw numbers only tell part of the story.

What's truly alarming is how agentic AI and attack automation services are democratizing sophisticated cybercrime. Where once only elite hackers could execute complex attacks, now anyone with a few hundred dollars can rent AI-powered tools that adaptively probe defenses, mimic human behavior, and scale attacks across thousands of targets simultaneously. Our data shows attack automation service usage jumped from 31% to 36% of all attacks in just one quarter.

This evolution demands a new defensive mindset. The old playbook of reactive security measures and static defenses no longer suffices when attackers leverage AI to continuously evolve their tactics. Every enterprise—regardless of industry or size—faces this escalating threat.

That's why we've created this comprehensive benchmark report. Inside, you'll find:

- Industry-agnostic trends revealing how fraudsters operate globally
- Deep dives into 9 major industries highlighting specific attack patterns
- Actionable intelligence to help you understand where your defenses stand relative to the broader threat landscape

Whether you're protecting a dating platform from romance scammers, or a fintech company protecting your customers from account takeovers, or a bank grappling with MFA compromise and AI-driven fake accounts, this data provides the context needed to make informed security investments. You'll see not just what's happening industry-wide, but how your specific sector compares.

The goal isn't to alarm, but to arm you with intelligence. By understanding scammer economics, timing patterns and tactical preferences, we can collectively work to make cybercrime unprofitable. Because when we disrupt their ROI, we protect not just our enterprises, but the consumers who trust us with their digital lives. Remember, if we don't make fraud unprofitable, we make it inevitable!

And as always, if you're staring down an urgent situation or have questions, just reach out to us directly.

Stay vigilant,

Frank Teruel
Chief Operating Officer
Arkose Labs

THE ATTACK LANDSCAPE

Today's scammers have more tools at their disposal than ever. They are globally active, launching both volumetric and low-and-slow targeted attacks.

In the onslaught of AI-powered cybercrime, no industry is spared. But by examining attack patterns like entry points, attack types, sizes and timings, security leaders can better understand the rhythms of the fraudsters targeting them.

This insight into scammer behavior is the first step in uncovering the motives of cybercriminals, in order to ultimately disrupt their economics and shut down their schemes. Armed with this intel, companies can move from a reactive to a proactive approach, adopting the security practices designed to detect and block fraudsters in real-time. With this kind of holistic behavior analysis, security professionals can see the big picture, building a blueprint of cybercriminals and their patterns.

This report analyzes Q2 2025 attack data and reveals critical shifts from Q1, providing essential benchmarks for your security posture.

Glossary

Attack: Deliberate attempt to breach digital defenses

Attack Point: Vulnerability targeted (sign-up, sign-in, etc.)

Attack Type: Specific fraud method (fake accounts, ATO, etc.)

Attack Mechanism: Tools used (bots, human fraud farms, etc.)

Attack Volume: Number of attack attempts

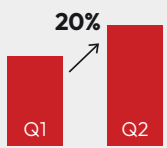
Attack Size: Size of attacks (composed of malicious traffic)

Malicious Traffic: Aggregate flow of fraudulent activities

Scam: Fraudulent scheme designed to deceive victims for financial gain or data theft

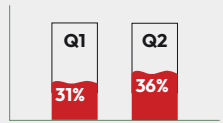
KEY FINDINGS

FRAUD KEEPS RISING



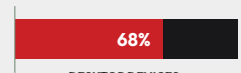
Q2 over Q1, malicious traffic increased nearly 20%; average attack size increased by more than 12%

SCAMMERS ARE STREAMLINING THEIR PROCESSES



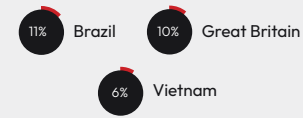
36% of attacks in Q2 were launched using attack automation services, up from 31% in Q1

DESKTOP DOMINANCE PERSISTS



68% of attacks originated from desktop devices, with Chrome maintaining overwhelming browser preference as fraudsters consolidate around mainstream options

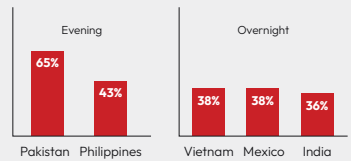
GLOBAL FRAUD HUBS EMERGE



Excluding U.S. traffic (often masked), Brazil leads at 11%, followed by Great Britain (nearly 10%) and Vietnam (6%).

ACCOUNT CREATION ATTACKS REMAIN RIFE

As observed last year, sign-up and sign-in flows were a major entry point, with three-quarters of scams starting this way



ROUND-THE-CLOCK OPERATIONS

Evening attacks dominate from Pakistan (65%) and the Philippines (43%), while overnight peaks originating in Vietnam (38%), Mexico (38%) and India (36%) suggest organized fraud rings working shifts

ATTACK POINTS

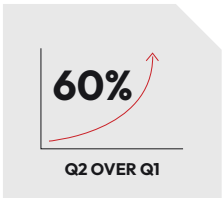
Attacks were concentrated in sign-up, demonstrating that creating new fraudulent accounts remains a primary strategy for fraudsters looking to infiltrate their targets. This shows that scammers continue to exploit streamlined sign-up processes, seeking the path of least resistance to launch synthetic identity scams, mule accounts and other types of fraud.

The second most utilized attack point was sign-in: a trend that held steady during every quarter last year. Account takeover scams can be highly lucrative for fraudsters. They might seek to take control of high value accounts and monetize valuable assets such as gift card balances. And targeting lower value accounts at scale is also a common tactic for criminals. Using bots, they can launch volumetric credential stuffing attacks designed to exploit low-friction flows and weak password hygiene.

SMS and account management were the other most observed attack points. We saw SMS fraud increase to make up 9% of all attacks in Q4 last year, and similar numbers in Q2 2025 suggests that the fraudsters that have implemented these scams within the last year continue to find them effective.

ATTACK TYPES

Fake account creation remained rife in Q2 2025, accounting for 48% of attacks. In some industries, these new accounts allow the cybercriminal to access benefits like loyalty points, referral credits and other bonuses, making account creation a remunerative way to start a scam.



Having gained entry, fraudsters can exploit the account in various ways. In-app scams are a growing attack type, with malicious traffic from this type of attack growing by over 60%, Q2 over Q1.

MFA compromise is another attack type where malicious traffic ballooned, increasing more than 400% Q2 over Q1. In these pernicious and increasingly prevalent attacks, fraudsters use convincing reverse-proxy phishing to spoof interactions with real websites, in order to steal session cookies.

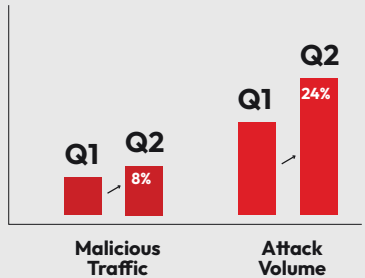
ATTACK MECHANISMS

Volumetric attacks continue to dominate the fraud landscape, with 85% of the Q2 2025 malicious traffic coming from bots. This is no surprise: these attacks are cheap and easy to execute for even inexperienced fraudsters relying on brute force. The success rate is low, but the high volume means that fraudsters can still make money through these attacks.

Conversely, attack automation services are often used to launch carefully constructed attacks. This attack mechanism is also on the rise: comparing Q2 over Q1, both the attack volume and malicious traffic associated with attack automation services increased.

AI is lowering the barrier to entry for more sophisticated attacks. With these services, including phishing kits, fraudsters are upping their game and constructing more refined attacks that are often effective in mimicking human behavior.

ATTACK AUTOMATION SERVICE



Attack automation service malicious traffic increased 8%, while its attack volume increased 24%

ATTACK BROWSERS & DEVICES

Top Browsers Used by Attackers

Fraudsters continue to favor mainstream browsers that offer the best balance of functionality and anonymity. The remarkable stability in top browser rankings—with the top 7 positions unchanged between quarters—suggests attackers have reached a relative equilibrium in their toolset preferences. Chrome maintains its position as the overwhelmingly preferred attack browser.

Significant Q2 Observations

- **Chrome Mobile iOS entered the top 10**, climbing from #11 to #9
- **Desktop Chrome variants expanded**, with browsers like Headless Chrome suggesting increased automation sophistication
- **Mobile browser fragmentation increased** to include browsers such as Opera Touch and Firefox Mobile iOS
- **Yandex Browser dropped out of the top 10** as attackers consolidated around more mainstream options
- **Specialized browsers showed volatility**, with Battle.net declining sharply while Twitter gained in mobile popularity

Mobile vs. Desktop Split

Desktop dominance remains absolute in the attacker ecosystem, with the platform split holding remarkably steady across Q1 (67% desktop, 33% mobile) and Q2 (68% desktop, 32% mobile). While legitimate users increasingly transact via mobile devices, fraudsters maintain their desktop preference for several operational reasons, including superior automation capabilities and more sophisticated proxy and VPN integration The stability in device distribution across quarters suggests this split represents an equilibrium point for current attack methodologies.

TOP 5 BROWSERS BY NUMBER OF ATTACKS, Q2 2025

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

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

ATTACK COUNTRY PATTERNS

Attack Distribution by Country of Origin

Our analysis of Q2 2025 attack data reveals that the United States continues to dominate raw traffic volumes at nearly 30% 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.

Across industries, the top 3 countries are Brazil (over 11%), Great Britain (nearly 10%) and Vietnam (over 6%).

Across Industries: Top 10 Attack Origins (Excluding U.S.)
Brazil
Great Britain
Vietnam
Germany
India
France
Philippines
Mexico
Indonesia
Turkey

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

ATTACK TIMING

Scammer Daily Activity Patterns, by Country of Origin

Analysis of attack timing patterns reveals distinct operational signatures that provide valuable insights into the human-operated nature of modern cybercrime. The data can demonstrate clear regional variations in attack timing that align with both local working patterns and strategic targeting of international victims.

But, as referenced earlier, location spoofing might be at play. Interestingly, the most popular time of day for Q2 2025 attacks that appear to come from the U.S. is the daytime (50%), whereas in Great Britain the leading time for attacks is the evening (48%). The reason for this could well be that a large amount of the attack traffic that seems to come from these countries is in fact coming from another country, attacking during the U.S. daytime which is also the evening in Europe. Where we see lots of traffic in the evenings, it suggests that fraudsters might be active after their day jobs. Countries that showed this pattern in Q2 include the Philippines (43%) and Pakistan (65%).

Meanwhile, countries that see more than one third of their attack traffic overnight include Vietnam (38%), Mexico (38%) and India (36%). It's possible that in these countries, the round-the-clock fraudulent traffic is connected with established cybercrime rings, working shifts to launch both volumetric and human-driven attacks.

- Morning/Afternoon: 8 a.m. - 4 p.m. Local Time
- Evening/Night: 4 p.m. - 12 a.m. Local Time
- Late Night/Early Morning: 12 a.m. - 8 a.m. Local Time

RECOMMENDED ACTIONS

Fortify Sign-Up Security

Account creation continues to be a primary access point for cybercriminals. Consider implementing behavioral biometrics to distinguish humans from the automation services now dominating attacks, and use passwordless solutions resistant to credential stuffing.

Neutralize Automation

Use of attack automation services by fraudsters is growing. Companies should stay vigilant, screening for large volumes of unusual traffic to stamp out these mass attacks. And, coaching employees and customers to spot and report phishing scams could help to shut down MFA compromise schemes faster.

Secure SMS

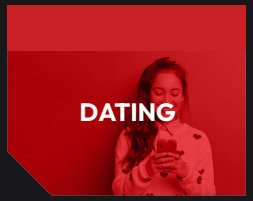
With 9% of attacks now at SMS flows, it's critical for cross-functional teams to carefully monitor SMS traffic volumes, requests and the associated geographies, drilling down into any anomalies.

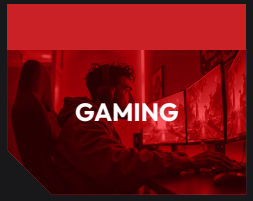
Protect Existing Accounts

Compromised accounts threaten to shatter customer trust. To prevent this, companies should deploy anomaly detection and session monitoring to protect against account takeover traffic targeting their platforms.

CHOOSE YOUR INDUSTRY

Every industry faces unique fraud challenges. While attack volumes and methods vary, one truth remains constant: fraudsters adapt their tactics to exploit sector-specific vulnerabilities. Select your industry below.





DATING INDUSTRY ATTACK LANDSCAPE

DATING INDUSTRY ATTACK POINTS

The dating industry experienced a pronounced shift in attacker behavior during Q2 2025. Sign-in activity intensified sharply, while SMS abuse decreased. One possible explanation is that compromising existing user accounts provides immediate access to trusted profiles and verified identities, reducing the need for attackers to create new accounts from scratch.

Sign-In Attacks: Concentrated Growth

Attacks: +44%	**Malicious traffic: +301%**	**Average attack size: +178%**

Sign-in malicious traffic grew significantly even as attack counts increased more moderately. The discrepancy between traffic and frequency indicates larger, more sustained activity within fewer attack events.

SMS Attacks: Decline in Activity

Malicious traffic: -28%	**Average attack size: −23%**

SMS-based malicious activity decreased in both frequency and scale, diverging from the modest growth seen in most other industries.

What This Reveals

The Q1→Q2 comparison shows a redistribution of malicious activity within the dating industry, with stronger concentration on authentication endpoints and reduced activity in SMS flows.

DATING INDUSTRY ATTACK TYPES

The dating industry experienced a dramatic surge in account takeover (ATO) attacks in Q2, with fraudsters increasingly focusing their efforts on compromising existing user accounts. One reason why: Existing accounts provide instant access to pre-established trust relationships and verified profiles—eliminating the time and effort associated with building fake accounts.

Account Takeover (ATO): Expanded and Intensified

Attacks: +44%	Malicious traffic: +301%	Average attack size: +178%

ATO remained the dominant threat for dating platforms. Malicious traffic grew 10x the industry-wide growth (+30%), with a significant rise in attack count and event size indicating heavier credential-stuffing and takeover operations.

SMS Toll Fraud: Lessening in Size and Frequency

Attacks: -6%	Malicious traffic: -28%	Average attack size: -23%

SMS-related abuse contracted across all measures, diverging sharply from the modest increases seen in other industries. The decline in both event frequency and malicious traffic suggests improved resilience or shifting attacker priorities away from messaging

What This Reveals

The Q2 data shows a clear redistribution of malicious activity toward credential-based takeover, while SMS abuse declined. With ATO traffic rising 301% quarter over quarter, dating remains one of the most concentrated verticals for this type of compromise.

DATING INDUSTRY ATTACK MECHANISMS

Dating platforms face a distinct attack mechanism landscape compared to other industries. While bots dominate the broader threat environment (63% of malicious traffic across all industries in Q2), dating apps see a markedly different pattern.

Attack Mechanism Distribution by Number of Attacks

- Attack Automation Services: 74% (up from 45% in Q1)
- Bots: 24% (down from 51% in Q1)
- Human Fraud Farms: 2% (down from 4% in Q1)

The dominance of attack automation services represents a dramatic shift from Q1, with these sophisticated tools surging by 93% in attack volume and 354% in malicious traffic. This explosion suggests fraudsters are investing in specialized toolkits designed specifically for dating platform attacks.

Quarter-Over-Quarter Changes:

- Attack Automation Services: +93% attacks, +354% malicious traffic
- Bots: -45% attacks, -46% malicious traffic
- Human Fraud Farms: -43% attacks, +55% malicious traffic

The shift from basic bots to automation services indicates an escalation in sophistication. These services often include features like:

- Advanced CAPTCHA solving capabilities
- Behavioral mimicry to avoid detection
- Coordinated multi-account management
- Automated conversation scripts for romance scams

What This Reveals

The decline in bot usage (-45%) doesn't indicate reduced threat levels. Rather, it shows fraudsters transitioning to different tools—whether that migration is driven by cost-effectiveness, capability, availability or additional motivations.

DATING INDUSTRY ATTACK BROWSERS & DEVICES

Browser patterns in dating attacks reveal a striking shift toward consolidation between Q1 and Q2, suggesting attackers are refining their technical approaches.

Key Patterns:

- Sharp reduction in browser diversity from Q1 to Q2
- Chrome maintained its dominant position
- Mobile Safari held strong second place
- Chrome Webview remained in third position

The dating industry shows a dramatic reversal in the devices attackers use to launch their campaigns, diverging sharply from broader industry patterns.

Attacks Shift From Desktop to Mobile

Fraudsters significantly changed their attack origination patterns:

- **Attacks via desktop:** Declined 16%
- **Attacks via mobile:** Surged 62%
- **Device distribution:** Flipped from 55% desktop/45% mobile to 39% desktop/61% mobile

This reversal contrasts starkly with the industry-wide pattern where attacks maintain an approximately 68% desktop/32% mobile split.

Why Fraudsters Moved to Mobile Infrastructure

The 61% increase in attacks originating from mobile devices aligns with the browser data showing Mobile Safari and Chrome Webview prominence. It suggests:

- **Mobile device farms:** Investment in physical devices or cloud-based emulators
- **App-specific tooling:** Attack automation services that run on mobile platforms Detection
- **evasion:** Security teams often expect attacks from desktop environments Authentication
- **exploitation:** Mobile sessions and app APIs may have different security postures

TOP 3 BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP AND MOBILE DEVICES – DATING INDUSTRY, Q2 2025

No.	Desktop
01	Chrome
02	Safari
03	Firefox

No.	Mobile
01	Mobile Safari
02	Chrome Webview
03	Chrome Mobile

DATING INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that traffic appearing to originate from the United States represents 41% of total dating industry 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 dating industry companies, these countries are Nigeria, Brazil and Germany.

Key Geographic Insights

The West African Connection: Nigeria's dominance at 9% aligns with well-documented romance scam operations originating from West Africa. Ghana also contributes to attack volumes, suggesting an established romance scam infrastructure across the region.

European Clusters: A notable concentration emerges in Western Europe, with Germany, France and Great Britain each contributing slightly more than 3% of attacks. Spain adds another roughly 2%, creating a significant European presence.

Latin American Operations: Brazil stands out at over 6%, with additional contributions from Mexico (over 1%) and Chile (just under 1%), indicating growing threat activity across Latin America.

Middle East and North Africa: Egypt's more than 3% share, combined with Saudi Arabia's just over 1%, suggests emerging threat centers in the MENA region.

Asian Presence: The Philippines, India, China and Hong Kong show more modest volumes compared to other regions.

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

	Nigeria
	Brazil
	Germany
	Egypt
	France
	Great Britain
	Spain
	India
	Philippines
	Mexico

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

DATING INDUSTRY RECOMMENDED ACTIONS

Fortify Authentication

Deploy adaptive authentication that scales with risk. Implement behavioral biometrics to distinguish humans from the automation services now dominating attacks. Consider passwordless solutions resistant to credential stuffing.

Neutralize Automation

Combat the 354% surge in attack automation service traffic with advanced challenges tuned specifically for dating platforms. Deploy proof-of-work systems that make mass attacks economically unfeasible.

Secure Mobile Channels

With 61% of attacks now mobile-originated, implement device fingerprinting to detect emulators and device farms. Monitor Chrome Webview traffic closely—it may indicate sophisticated app-mimicking attacks.

Geographic Risk Scoring

Use enhanced verification for high-risk regions such as Nigeria.

Protect Existing Accounts

Compromised accounts offer instant access to trust relationships. Deploy anomaly detection and session monitoring to protect against the surge in account takeover traffic targeting dating platforms specifically.

▶ Jump to Report Conclusion

FINTECH INDUSTRY ATTACK LANDSCAPE

FINTECH INDUSTRY ATTACK POINTS

Fintech platforms recorded the largest relative growth in malicious traffic across all sectors, concentrated in account creation and account management functions. This concentration may reflect the continuing appeal of fintech targets, where successful compromise can yield direct financial benefit or access to verified payment credentials.

Sign-Up Attacks: Substantial Growth

Attacks: +26%	Malicious traffic: +478%	Average attack size: +358%

Sign-up malicious traffic increased more than 17x the industry-wide average (+27%), while attack volume rose modestly. The data indicates a higher level of intensity within each event.

Account Management: Expanded Post-Authentication Activity

Malicious traffic: +302%	Share of attacks: 9%→17%

Malicious traffic on the account management flow grew more than 4x the cross-industry average (+70%), more than tripling its share of overall fintech activity.

Sign-In: Decline in Line With Market Averages

Malicious traffic: –33%	Industry-wide change: –31%

Sign-in activity declined at a rate similar to the cross-industry averages but remained the dominant attack point, accounting for just above half of all fintech attacks.

What This Reveals

The Q2 data shows heightened emphasis on account-creation and management layers, where growth far exceeded industry baselines. This pattern suggests that attackers perceive increased value in targeting areas tied to verification, credential storage and transactional control.

FINTECH INDUSTRY ATTACK TYPES

The fintech industry saw large shifts in attack behavior in Q2 2025, with spikes in fake account creation and in-app abuse. It's not surprising—fraudsters continue to pursue the quickest path to verified payment credentials and stored financial data.

In-app threats: Expanded Post-Authentication Activity

Attacks: +156%	Malicious traffic: +302%	Average attack size: +57%

In-app threats experienced broad growth across all measures, with traffic rising 5x the in-app threats industry growth of +60%.

Fake Account Creation: Substantial Escalation

Attacks: +19%	Malicious traffic: +659%	Average attack size: +539%

Fake account creation grew at an even faster rate, with malicious traffic surging over sixfold quarter over quarter. The large gap between traffic and frequency points to higher-intensity automation within onboarding flows.

Account Takeover (ATO): Traffic Decline Despite Volume Increase

Attacks: +26%	Malicious traffic: –33%	Average attack size: –47%

Although the number of ATO events increased, the total malicious traffic dropped by one-third. The decline in average attack size suggests smaller-scale credential attacks following Q1's heavier activity.

SMS Toll Fraud: Modest Growth From a Low Base

Attacks: +33%	Malicious traffic: +59%	Average attack size: +19%

SMS-related threats rose across all dimensions but remained a relatively small proportion of total fintech activity.

What This Reveals

Fintech's Q2 data highlights significant pressure on account creation and account management. With fake account creation and in-app threats growing at multiples of the cross-industry growth rate, attackers appear to be concentrating efforts where financial credentials and transaction capabilities are most accessible.

FINTECH INDUSTRY ATTACK MECHANISMS

The tools fraudsters use to execute attacks reveal a surprising inversion of industry trends, with fintech experiencing fundamentally different pressures than other sectors. While bots comprise 61% of all fintech attacks, bot malicious traffic grew just 7% in Q2—far below the industry-wide surge of 22%.

Growth for Attack Automation Services and Human Fraud Farms

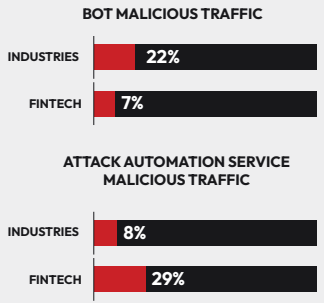
Attack automation services showed moderate but concerning increases. These sophisticated tools grew 29% in malicious traffic, nearly 4x the industry rate of 8%. Despite their share of attacks decreasing from 41% to 37%, attack automation services are generating more traffic per attack.

Another striking finding? Human-operated attacks exploded 231% in malicious traffic, though they remain just 3% of total attacks.

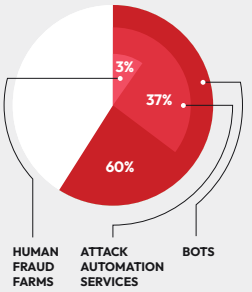
Attack Distribution (Q2)

- Bots: 60% (dominant but slower growing)
- Attack automation services: 37% (declining share but accelerating traffic)
- Human fraud farms: 3% (tiny share but massive growth)

QUARTER OVER QUARTER GROWTH



ATTACK DISTRIBUTION (Q2)



What This Reveals

One possible explanation for the small bot traffic growth? Fintech's bot defenses may be more effective than average, forcing fraudsters to seek alternative methods. Meanwhile, the explosive growth rate for malicious traffic from human fraud farms suggests fraudsters are willing to invest in more resource-intensive attack methods when targeting fintech platforms.

FINTECH INDUSTRY ATTACK BROWSERS & DEVICES

Browser patterns in attacks reveal notable consolidation, with Chrome maintaining overwhelming dominance while mobile browsers show significant growth.

Notable Browser Findings

- In Q2, top 3 browsers account for 79% of all attacks
- Chrome Mobile, Mobile Safari and Chrome Webview showed strong growth
- Several Q1 browsers (Battle.net, WeChat, Headless Chrome) disappeared entirely

Device Distribution Shifts Toward Mobile

- **Attacks via desktop:** Grew 24%
- **Attacks via mobile:** Surged 57%
- **Device distribution:** Fom 62% desktop/38% mobile to 56% desktop/44% mobile

This 6 percentage point swing toward mobile contrasts with the industry-wide pattern of approximately 68% desktop/32% mobile with minimal quarter-over-quarter change.

What This Reveals

The surge in mobile-originated attacks—more than double desktop's growth—signals fraudsters are expanding mobile attack infrastructure and investing in tools that mimic mobile app traffic patterns.

TOP 5 BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP AND MOBILE DEVICES – FINTECH INDUSTRY, Q2 2025

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

No.	Mobile Browsers
01	Chrome Mobile
02	Mobile Safari
03	Chrome Webview
04	Chrome
05	Chrome Mobile iOS
05	UC Browser

FINTECH INDUSTRY ATTACK COUNTRY PATTERNS

Attack geography data reveals that Great Britain dominates fintech attacks at nearly 44% of total volume, with the United States showing surprisingly low representation at just under 13%—a stark contrast to the typical U.S. dominance seen across other industries.

When examining the geographic distribution, several distinct patterns emerge.

Great Britain Dominance: Great Britain's exceptional share represents an unusual concentration for fintech attacks. This may reflect its position as a global financial hub, making these IP addresses attractive for fraudsters targeting financial services.

The U.S. Anomaly: The United States shows dramatically lower attack volumes than the industry norm where U.S. traffic typically dominates. This suggests fraudsters may be using different location-masking strategies when targeting fintech versus other sectors.

South Asian Presence: Pakistan emerges as the third-largest source of attacks, representing a significant concentration relative to its typical presence in other industries.

Global Distribution: The data shows attacks originating from a wide range of countries, indicating a globally distributed threat landscape with fraudsters operating from diverse locations spanning Europe, Asia, Africa and the Americas.

Fintech Industry: Top 10 Attack Origins	
	Great Britain
	United States
	Pakistan
	Brazil
	Algeria
	Germany
	Vietnam
	Kenya
	Ukraine
	Netherlands

FINTECH INDUSTRY RECOMMENDED ACTIONS

Harden Account Creation

Deploy multi-layered verification at sign-up that scales with risk signals. The 478% surge in demands enhanced KYC measures including document verification, biometric checks and behavioral analysis during onboarding.

Counter Fake Account Explosion

Implement graph-based fraud detection to identify connected accounts, deploy velocity checks on payment method reuse and monitor for synthetic identity patterns across your platform.

Secure Mobile Channels

Given the growth in mobile-originated attacks, implement advanced device fingerprinting to detect emulators and device farms. Monitor for browser anomalies that signal attack tool usage.

Geographic Intelligence

Use risk-based authentication that considers geographic patterns—Great Britain leads at 44%, with Pakistan also showing disproportionate activity at 11%.

Maintain Authentication Vigilance

While ATO decreased 33% in malicious traffic, it represents 54% of all fintech attacks. Deploy risk-based MFA, continuous authentication and behavioral anomaly detection to preserve defensive gains.

▶ Jump to Report Conclusion

GAMING INDUSTRY ATTACK LANDSCAPE

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

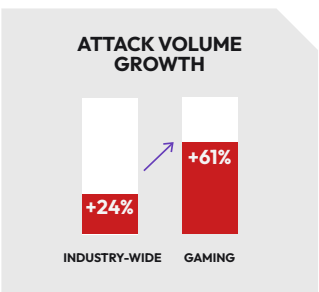
Attack automation services surged 61% in volume—2.5x higher than the industry-wide 24% increase. These services grew from 15% to 25% of all gaming attacks, indicating fraudsters are investing in professional automation platforms alongside traditional bot operations. Meanwhile, bot attacks fell 11% in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

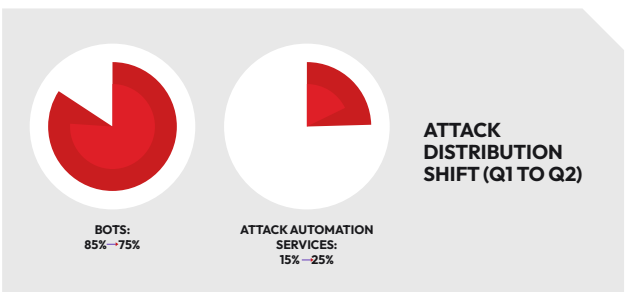
Attack Distribution Shift (Q1 to Q2):

- 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.

GIG ECONOMY INDUSTRY ATTACK LANDSCAPE

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% averageattack size
- **Bots:** +23% attacks, -35% malicious traffic, -47% average attack size
- **Human fraud farms:** -87% attacks, -93% malicious traffic, -48% average attack

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

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.

Jump to Report Conclusion

MEDIA INDUSTRY ATTACK LANDSCAPE

MEDIA INDUSTRY ATTACK POINTS

Streaming media platforms experienced broad expansion in attack activity during Q2 2025, with attacks growing 48% overall. The most substantial changes occurred in account management and sign-up.

Account Management: Significant Growth in Attack Frequency

Attacks: +212%

Account management attacks increased more than 3x, representing the largest proportional change among media attack points. This concentration suggests attackers are targeting user-level settings, subscription controls and content access mechanisms.

Sign-Up: Substantial Increase

Attacks: +800%

Sign-up activity grew dramatically in frequency, though it remained a relatively small portion of overall attack volume.

Sign-In: Moderate Growth

Attacks: +29%

Sign-in attacks increased modestly, maintaining their position as the dominant attack vector at 75% of all media attacks.

What This Reveals

The media and streaming sector experienced a redistribution of attack activity, with pronounced growth in account management functions. This pattern suggests sustained targeting of user-level controls and authenticated session abuse.

MEDIA INDUSTRY ATTACK TYPES

Media and streaming platforms saw one of the most dramatic increases in attack activity across all industries in Q2 2025. Subscription and streaming services hold stored payment credentials and valuable digital entitlements, making authenticated accounts a high-value target for attackers.

In-App Threats: Major Surge in Authenticated Abuse

Attacks: +213%

Attack counts more than tripled quarter over quarter, marking the largest increase of any attack type within the sector. The sustained escalation indicates intensified probing of account entitlement and subscription endpoints.

Account Takeover (ATO): Moderate but Steady Growth

Attacks: +27%

ATO activity increased slightly, continuing the broader trend of targeted credential testing and token-based access. While growth was less extreme than in-app threats, takeover campaigns remained a core threat vector for streaming services.

Fake Account Creation: Sharp Increase From a Low Base

Attacks: +800%

New account abuse expanded sharply, though from a small starting volume. The spike likely reflects opportunistic automation during free trial or promotional windows.

What This Reveals

Media and streaming platforms experienced an unmistakable rise in authenticated and account access attacks. The Q2 surge in in-app and account creation attacks reinforces how stored payment methods and subscription credentials continue to drive attacker focus in this vertical.

MEDIA INDUSTRY ATTACK MECHANISMS

Media and streaming platforms experienced significant growth across all attack mechanisms in Q2 2025, including a 95% jump in average attack size. Bots maintained dominance despite substantial gains by automation services.

Attack Distribution

- **Bots:** 53% of attacks (up from 44% in Q1)
- **Attack automation services:** 45% of attacks (down from 55% in Q1)
- **Human fraud farms:** 2% of attacks (consistent with Q1)

Quarter-Over-Quarter Changes

- **Attack automation services:** +21% attacks, +52% malicious traffic, +26% average attack size
- **Bots:** +78% attacks, +248% malicious traffic, +95% average attack size
- **Human fraud farms:** +200% attacks, -2% malicious traffic, -67% average attack size

What This Reveals

Media platforms saw bots surge dramatically in Q2, with attack volume growing more than 11x the cross-industry bot traffic growth rate. This extraordinary bot traffic increase indicates attackers deployed significantly larger volumetric campaigns against streaming services.

Despite declining as a proportion of total attacks, automation services grew substantially in both frequency and traffic, suggesting continued investment in sophisticated tooling. Meanwhile, human fraud farms tripled in frequency but generated essentially flat traffic, indicating smaller manual operations.

Q1→Q2 MALICIOUS TRAFFIC GROWTH RATES

MEDIA INDUSTRY ATTACK BROWSERS & DEVICES

Extreme Chrome Concentration

Chrome captured 55% of streaming media attacks in Q2, maintaining its dominant position from Q1. Chrome variants collectively account for over 70% of browser signatures, suggesting attackers optimize for the dominant browser ecosystem.

Mobile App Attack Vectors Emerge

Chrome Webview jumped from 4% in Q1 to 15% in Q2—the most significant change in the browser distribution. This embedded browser, typically used within mobile applications, indicates a shift toward attacks originating from or mimicking streaming app traffic rather than traditional web browsers.

Device Distribution Shifts Toward Mobile

While overall attacks grew 48%, fraudsters expanded their mobile attack capabilities disproportionately.

- **Attacks via desktop:** Grew 33%
- **Attacks via mobile:** Grew 67%
- **Distribution:** Shifted from 74% desktop/26% mobile to 69% desktop/31% mobile

Key Takeaway

The surge in mobile-originated attacks—double desktop's growth rate—combined with Chrome Webview's dramatic rise signals fraudsters are investing heavily in mobile attack infrastructure. The prominence of Chrome Webview in mobile-originated attacks suggests sophisticated attack tools that can mimic app-based traffic patterns, representing a strategic evolution in how attackers target streaming services.

TOP 5 BROWSERS BY NUMBER OF ATTACKS, MEDIA INDUSTRY, Q2 2025

No.	Desktop Browsers
01	Chrome
02	Firefox
03	Microsoft Edge
04	Safari
05	Headless Chrome

No.	Mobile Browsers
01	Chrome Webview
02	Mobile Safari
03	Chrome
04	Chrome Mobile
05	Samsung Broswer

MEDIA INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that traffic appearing to originate from the United States represents 37% of total streaming media industry 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 media companies, these countries are Brazil and Germany (tied), followed by Argentina.

Key Geographic Insights

South American Operations: Brazil leads non-U.S. attack traffic at just over 6%, with Argentina contributing nearly 5%. Colombia (3%), Venezuela (2%), and smaller contributions from Ecuador, Peru, Chile and Uruguay indicate established fraud operations across South America.

European Distribution: Germany leads Europe with 7% of apparent attacks, while France contributes nearly 5%. Italy, Netherlands, Poland and smaller volumes from other European nations show widespread activity.

Asian Presence: India shows 3% of attacks, with Philippines (2%), Indonesia (1%) and smaller volumes from other Asian countries. This represents moderate Asian activity in media platform attacks.

Commonwealth and Other Regions: Serbia emerges with 2%, while Turkey also contributes 2%. Smaller volumes appear from Australia, Belgium, Cyprus and various other nations.

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

	Brazil
	Germany
	Argentina
	France
	Italy
	India
	Colombia
	Netherlands
	Philippines
	Poland

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

MEDIA INDUSTRY RECOMMENDED ACTIONS

Secure Authenticated Sessions

Deploy session monitoring, anomaly detection for subscription changes and behavioral analysis to protect account entitlements and stored payment methods. Focus on detecting abuse within authenticated environments where fraudsters can modify subscriptions and billing details.

Combat Volumetric Bot Campaigns

Enhance bot detection tuned specifically for streaming services' access patterns. The extraordinary surge in bot traffic, combined with dramatically larger attack sizes, demands defenses capable of handling intense volumetric pressure.

Validate Mobile Infrastructure

Implement device fingerprinting to detect emulators and tools mimicking streaming app traffic. Chrome Webview's sudden prominence suggests fraudsters are developing new attack methodologies specifically targeting mobile applications.

Monitor Account Creation Spikes

Deploy velocity controls on trial sign-ups, email verification and payment method validation to limit promotional abuse. Fraudsters continue exploiting free-trial and promotional windows despite improved entry-point defenses.

Regional Risk Assessment

Apply enhanced verification for subscription changes from high-risk regions, particularly when combined with unusual viewing patterns or rapid device changes. Note that Brazil, Germany and Argentina lead non-U.S. attack concentrations.

▶ Jump to Report Conclusion

OTA INDUSTRY ATTACK LANDSCAPE

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 MECHANISM

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.

Jump to Report Conclusion

RETAIL INDUSTRY ATTACK LANDSCAPE

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

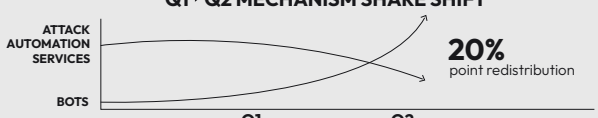
What This Reveals

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 Takeaway

The combination of extreme Chrome consolidation and the dramatic pivot to mobile suggests retail fraudsters are rapidly adapting their infrastructure to match legitimate consumer behavior, where mobile commerce increasingly dominates. This transformation from 30% mobile to 47% mobile in a single quarter represents one of the fastest tactical shifts observed across any industry sector.

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.

Jump to Report Conclusion

SOCIAL MEDIA INDUSTRY ATTACK LANDSCAPE

SOCIAL MEDIA INDUSTRY ATTACK POINTS

Social platforms recorded rising activity in account management and SMS-based events in Q2 2025, while attacks on sign-in and sign-up points declined. This may indicate a shift in focus toward account control and verification abuse within existing user sessions.

Account Management: Growth Above Industry Average

Attacks: +61%	**Malicious traffic: +105%**	**Average attack size: +27%**

Account management malicious traffic more than doubled, significantly outpacing the industry-wide account management growth of +70%.

SMS: Higher Traffic and Average Size

Attacks: +17%	**Malicious traffic: +277%**	**Average attack size: +223%**

Malicious SMS activity increased substantially in both scale and throughput.

Sign-In and Sign-Up: Declines Across Entry Points

Sign-in attacks: –17%	**Sign-in malicious traffic: –75%**	**Sign-up attacks: –24%**	**Sign-up malicious traffic: –15%**

Both entry points recorded reduced activity compared with Q1 2025.

What This Reveals

Social media platforms experienced concentrated growth in post-authentication vectors and lower activity at entry points. This balance reflects a reallocation of effort toward ongoing account control and verification channels.

SOCIAL MEDIA INDUSTRY ATTACK TYPES

Social media platforms saw a mixed attack landscape in Q2 2025, with strong growth in in-app threats and sharp declines in both account takeover (ATO) and fake account creation. One likely explanation? Improved login and registration defenses appear to be pushing attackers to exploit authenticated environments and messaging-based systems instead.

In-App threats: Fastest-Growing Vector

Attacks: +61%	Malicious traffic: +105%	Average attack size: +27%

In-app threats more than doubled in traffic and grew strongly in frequency. This may reflect increasing focus on profile modification, content posting and session-based abuse—activity that occurs after an account is successfully authenticated.

Account Takeover (ATO): Continued Decline

Attacks: –21%	Malicious traffic: –73%	Average attack size: –65%

Fake Account Creation: Reduced Registration Abuse

Attacks: –24%	Malicious traffic: –15%	Average attack size: +11%

Registration-based fraud decreased across most metrics. The small uptick in average size suggests that remaining campaigns are more deliberate, possibly leveraging higher-quality data sources.

SMS Toll Fraud: Resurgence in Messaging Fraud

Attacks: +17%	Malicious traffic: +277%	Average attack size: +223%

Messaging-related abuse spiked in both frequency and scale, signaling a pivot toward exploiting verification or one-time passcode systems as other defenses strengthened.

What This Reveals

Q2 results show that social media threats are shifting deeper into authenticated and verification flows. As overt credential attacks slow, attackers are adapting through session-level abuse and messaging channel exploitation.

SOCIAL MEDIA INDUSTRY ATTACK MECHANISMS

Social media platforms experienced an overall contraction in attack activity during Q2 2025, with divergent trends across mechanisms as bot usage declined while attack automation services held steady.

Attack Distribution

- **Bots:** 62% of attacks (down from 70% in Q1)
- **Attack automation services:** 37% of attacks (up from 29% in Q1)
- **Human fraud farms:** 1% of attacks (up from <1% in Q1)

Quarter-Over-Quarter Changes

- **Attack automation services:** +1% attacks, -4% malicious traffic, -5% average attack size
- **Bots:** -29% attacks, -33% malicious traffic, -6% average attack size
- **Human fraud farms:** +200% attacks, +412% malicious traffic*, +71% average attack size*

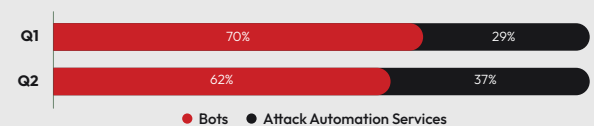
*Human fraud farm percentages reflect growth from an extremely small baseline, making percentage changes less meaningful.

What This Reveals

Social media platforms stood apart as one of the few industries where overall attack volume declined, driven primarily by a drop in bot attacks. This contraction diverges sharply from the cross-industry pattern where bot attacks remained relatively flat while bot traffic grew +22%.

Attack automation services maintained remarkable stability with near-zero growth in attacks and minimal traffic decline. This consistency—while cross-industry attack automation service attacks grew nearly one-fourth—suggests social media platforms may have reached an equilibrium state where attack automation service usage neither expands nor contracts significantly. This warrants close monitoring in future quarters.

Attack Distribution



SOCIAL MEDIA INDUSTRY ATTACK BROWSERS & DEVICES

Browser fingerprinting in social media shows the influence of platform-specific access methods, with native app browsers and mobile variants fragmenting what would otherwise be a Chrome-dominated landscape.

Chrome Dominance Despite Platform Diversity

Chrome was the browser signature in over 60% of social media attacks in Q2. Platform-specific browsers like Twitter and WeChat appear in the data but represent less than 5% combined, distinguishing social media from other industries more by their presence than their volume.

Mobile Browser Consolidation

Chrome Mobile dropped slightly from over 12% in Q1 to 11% in Q2, while Mobile Safari fell by roughly one-third. However, the emergence of Opera Touch and multiple Firefox mobile variants (Firefox Mobile, Firefox Mobile iOS) indicates diversification within mobile attack vectors rather than simple consolidation.

Platform-Specific Attack Indicators

Gaming-related browsers like Roblox, which represented nearly 4% of social media attacks in Q1, essentially disappeared by Q2. Platform-specific browsers (Twitter, WeChat, LinkedIn) remained present, suggesting different browser strategies for social media attacks.

Stable Device Distribution

Device distribution shifted slightly from 68% desktop/32% mobile to 70% desktop/30% mobile. This minimal point change aligns closely with the cross-industry baseline of 68% desktop/32% mobile, suggesting attackers maintain consistent infrastructure preferences for social media targets without significant tactical shifts.

TOP 5 BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP AND MOBILE DEVICES – SOCIAL MEDIA, Q2 2025

No.	Desktop Browsers
01	Chrome
02	Microsoft Edge
03	Firefox
04	Safari
05	Brave

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

SOCIAL MEDIA INDUSTRY ATTACK COUNTRY PATTERNS

Our analysis of Q2 2025 attack data reveals that traffic appearing to originate from the United States represents 36% of total social media 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 social media platforms, these countries are Brazil, Vietnam and Turkey.

Key Geographic Insights

Latin American Operations: Brazil appears to originate 13% of non-U.S. attack traffic, with Mexico contributing 4%. Smaller contributions from Argentina, Venezuela, Colombia and other Latin American nations indicate established but Brazil-centric operations in the region.

Southeast Asian Concentration: Vietnam shows as the origin for 11% of attacks, with Indonesia appearing to contribute nearly 4%. Malaysia, the Philippines and Thailand add to the Southeast Asian presence, suggesting coordinated regional operations.

Middle Eastern and South Asian Activity: Turkey appears to originate 5% of attacks, while India shows nearly 4% and Pakistan nearly 1%. This corridor shows moderate but consistent attack origins targeting social media platforms.

European Distribution: Great Britain appears to originate over 2% of attacks, with France, Germany, Italy, the Netherlands and smaller volumes from other European nations indicating dispersed but persistent activity.

Social Media: Top 10 Attack Origins (Excluding U.S.)

	Brazil
	Vietnam
	Turkey
	Mexico
	India
	Great Britain
	Indonesia
	Canada
	Germany
	Hong Kong

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

SOCIAL MEDIA INDUSTRY RECOMMENDED ACTIONS

Secure Account Management

Deploy monitoring for profile modifications, content posting abuse and session-based exploitation that occurs after successful authentication. Malicious activity is shifting deeper into authenticated flows even as overall attack volume declines.

Combat SMS Toll Fraud Resurgence

Implement SMS velocity limits, geographic risk scoring for phone numbers and alternative verification methods. Messaging-related abuse has spiked dramatically, signaling a pivot toward exploiting verification and one-time passcode systems as other defenses strengthen.

Maintain Authentication Vigilance

Continue investment in authentication security even as attack pressure temporarily decreases—fraudsters often return with evolved tactics. The current decline in sign-in attacks doesn't indicate reduced interest; rather, it suggests attackers are regrouping and retooling.

Monitor Mechanism Equilibrium

Monitor closely for any mechanism shifts that signal tactical evolution. Automation services held remarkably stable while bots declined—a unique equilibrium among industries analyzed that suggests social media platforms may have reached a steady state that warrants careful observation.

Geographic Risk Intelligence

Apply enhanced verification for account changes from high-risk regions, particularly when combined with unusual usage patterns. Note that Brazil leads non-U.S. attacks, followed by Vietnam and Turkey, indicating established Latin American and Southeast Asian fraud operations targeting social platforms.

▶ Jump to Report Conclusion

TECHNOLOGY INDUSTRY ATTACK LANDSCAPE

TECHNOLOGY INDUSTRY ATTACK POINTS

Technology platforms showed higher traffic growth in payment and sign-up activity during Q2 2025, alongside reductions in account management and sign-in attacks. This distribution may correspond with heavier emphasis on transactional systems and credential-based access.

Payment: Larger Events, Higher Traffic

Attacks: +0%	Malicious traffic: +281%	Average attack size: +281%

Malicious traffic increased substantially despite no change in attack count, producing significantly larger average event sizes.

Sign-Up: Continued Growth

Attacks: +23%	Malicious traffic: +47%	Average attack size: +19%

Sign-up activity grew steadily in both frequency and total traffic, aligning with the sector's broader increase in access-related activity.

Account Management and Sign-In: Declines Across Both Vectors

Account management: –52% attacks	Malicious traffic: –86%	Sign-in: –87% attacks	Malicious traffic: –35%

Both attack points declined in overall frequency, with sign-in events becoming larger on average.

What This Reveals

The Q2 data shows that malicious activity within technology platforms became more concentrated in payment and sign-up functions, while account management and sign-in activity decreased. The increase in payment traffic suggests continued targeting of areas tied to transaction execution and access provisioning.

TECHNOLOGY INDUSTRY ATTACK TYPES

The technology sector experienced mixed attack patterns in Q2 2025, with drops in in-app and account takeover activity but renewed growth in fake account creation. Attackers appear to be reallocating resources toward registration and access testing as platform defenses likely tighten around authentication.

In-app threats: Notable contraction in activity

Attacks: −52%	Malicious traffic: −86%	Average attack size: −71%

In-app threats declined sharply across all measures. The reduction indicates a slowdown in post-authentication exploitation, possibly reflecting the impact of strengthened session and permission controls.

Account takeover (ATO): Significant reduction in frequency

Attacks: −87%	Malicious traffic: −35%	Average attack size: +388%

Although ATO attacks fell substantially, the dramatic rise in average attack size shows that when campaigns did occur, they were highly concentrated. This pattern suggests more focused, resource-intensive efforts against specific high-value credentials.

Fake Account Creation: Renewed growth from steady baseline

Attacks: +23%	Malicious traffic: +47%	Average attack size: +19%

Registration abuse rebounded modestly in Q2, with increases across all metrics. The pattern points to persistent testing of onboarding and access-creation workflows even as other attack types waned.

What This Reveals

Q2 activity in the technology sector shows a redistribution of attacker effort toward smaller, targeted operations. Broad exploitation declined, while niche campaigns—particularly those tied to account registration and selective credential testing—remained active. Card testing continued to appear sporadically but at volumes too low to materially influence the overall trend.

Technology Industry Attack Mechanisms

Technology platforms experienced broad growth across attack mechanisms in Q2 2025, with bots maintaining dominant share.

Attack Distribution

- **Bots:** 68% of attacks (up from 64% in Q1)
- **Attack automation services:** 31% of attacks (down from 35% in Q1)
- **Human fraud farms:** <1% of attacks

Quarter-Over-Quarter Changes

- **Attack automation services:** +7% attacks, +22% malicious traffic, +14% average attack size
- **Bots:** +25% attacks, +51% malicious traffic, +21% average attack size
- **Human fraud farms:** -20% attacks, -92% malicious traffic*, -90% average attack size*

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

What This Reveals

Technology platforms saw synchronized growth across both bots and automation services, with bot traffic growing more than double the cross-industry bot growth.This substantial bot traffic increase, combined with a jump in average bot attack size, indicates attackers deployed larger, more intensive volumetric campaigns against technology targets in Q2.

Attack automation services attacks grew modestly in both frequency and traffic, aligning closely with cross-industry trends.

The mechanism distribution remained relatively stable compared to industries like retail or gig economy, which experienced 20+ percentage point swings. This consistency suggests technology platforms face established, steady-state fraud operations without dramatic tactical pivots.

Attack Distribution

TECHNOLOGY INDUSTRY ATTACK BROWSERS & DEVICES

Desktop Chrome Supremacy

Desktop Chrome alone was used in 67% of all technology sector attacks. This dominance distinguishes technology from many sectors where attacks are more distributed across browser types.

Consolidating Browser Landscape

Attacks heavily concentrated in mainstream options. Gaming-related browsers like Roblox and specialty browsers (Galeon, Hi Browser) essentially disappeared between quarters. Other platform-specific browsers remain minimal—WeChat appears at just 1% and development-related signatures like Atom at 0.2%. This suggests:

- Standardization of attack approaches
- Possible effectiveness of desktop-focused strategies
- Abandonment of niche attack vectors

Desktop Growth Outpaces Mobile

The technology sector experienced growth in both desktop- and mobile-originated attacks while moderately shifting toward desktop infrastructure. Device distribution shifted from 70% desktop/30% mobile to 76% desktop/24% mobile. This shift toward desktop moves technology further from the industry baseline of 67% desktop/33% mobile, indicating a moderate preference for desktop attack infrastructure.

TOP 5 BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP AND MOBILE DEVICES – TECHNOLOGY INDUSTRY, Q2 2025

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

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

TECHNOLOGY INDUSTRY ATTACK COUNTRY PATTERNS

Q2 2025 attack data reveals concentrated attack patterns from specific geographic regions targeting technology companies. Brazil leads apparent attack origins, followed by the United States and Russia. Unlike many other industries where U.S. traffic dominates due to location masking, this more balanced distribution suggests a genuinely global threat landscape with established attack infrastructure across multiple regions.

Key Geographic Insights

Latin American Operations: Brazil leads all apparent attack origins at over 26%, with Mexico contributing over 3% and smaller volumes from Argentina, Chile and Peru. This Latin American concentration, particularly Brazil's dominance, indicates established infrastructure targeting technology platforms.

Asian Presence: China shows over 6% of attacks, with India at nearly 3%. Japan, Malaysia and Vietnam contribute smaller volumes. The relatively modest Asian presence is notable given the region's technical infrastructure.

European Distribution: France appears to originate over 5% of attacks, with Great Britain and Netherlands each hovering above 2%. Germany, Italy and various other European nations show consistent but dispersed activity across the continent.

Middle Eastern Activity: Morocco stands out at 1.6%, with smaller contributions from the broader region including Turkey. This represents emerging threat activity from the MENA region.

Technology Industry: Top 10 Attack Origins	
	Brazil
	United States
	China
	France
	Russia
	Mexico
	India
	Great Britain
	Netherlands
	Indonesia

TECHNOLOGY INDUSTRY RECOMMENDED ACTIONS

Fortify Payment Systems

Implement transaction monitoring, behavioral analysis and anomaly detection specifically tuned for technology platform payment flows. The dramatic concentration of massively larger events on payment endpoints demands focused defensive resources where fraudsters are applying their most intensive pressure.

Counter Intensified Bot Campaigns

Enhance bot detection with adaptive challenges that scale with attack intensity. Bot malicious traffic grew at more than double the cross-industry growth rate, with substantially larger average attack sizes indicating attackers deployed more intensive volumetric campaigns against technology targets.

Secure Registration Flows

Deploy multi-layered verification including email validation, phone verification and behavioral analysis during account creation. Fake account creation rebounded with persistent testing of onboarding workflows, showing attackers maintain interest in registration abuse despite improved defenses.

Monitor Desktop Preference

Enhance desktop-based behavioral analysis. Technology platforms shifted further toward desktop attacks, moving away from the industry baseline, with desktop attacks growing at twice the mobile rate, suggesting desktop tools offer advantages when targeting technology companies.

Address Global Threat Distribution

Develop region-specific risk modeling for this genuinely global threat landscape with established infrastructure across Latin America, Eastern Europe and Asia. Brazil leads, followed by the U.S. and Russia—a notably balanced distribution unlike industries where the U.S. dominates due to location masking.

Jump to Report Conclusion

CONCLUSION

The Q2 2025 threat landscape reveals an inflection point in the evolution of cybercrime. The real transformation lies in how AI-powered attack automation services are fundamentally changing who can launch sophisticated attacks and at what scale. This shift demands a corresponding evolution in defensive strategy—from reactive measures to proactive disruption of attacker economics.

The data across these nine industries reveals distinct patterns that help you answer critical questions: Are we facing typical industry pressure, or targeted attacks? Where are our defenses holding, and where are they being systematically probed? Which attack vectors are growing, and which are declining as fraudsters reallocate resources?

The goal isn't simply to detect and block attacks. It's to make cybercrime unprofitable. When companies implement adaptive security that scales friction with risk, deploy behavioral biometrics that distinguish humans from sophisticated automation and secure the specific attack points most relevant to their industry, they don't just protect their platforms—they actively disrupt the economics that make fraud operations viable.

By understanding scammer behavior, timing patterns and tactical preferences revealed in this report, you can move from reactive security to proactive defense—protecting not just your company, but the consumers who trust you with their digital lives.

ABOUT ARKOSE LABS

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.

ACTIR

The Arkose Cyber Threat Intelligence Research (ACTIR) unit is a dedicated and specialized counterintelligence team embedded in Arkose Labs. Composed of full-time experts in cyber threat analysis, digital forensics and cybersecurity operations, ACTIR's primary mission is to identify, assess and neutralize sophisticated cyber threats. By leveraging cutting-edge technologies and methodologies, ACTIR provides actionable intelligence and orchestrates coordinated responses to mitigate threats posed by entities like Veiled Marble and Greasy Opal. Recently it partnered with Microsoft DCU and law enforcement to disrupt Vietnamese threat actor group Storm-1152…twice. Through collaboration with Arkose Labs' award-winning SOC, ACTIR plays a pivotal role in enhancing the cybersecurity posture and ensuring the integrity of the digital infrastructure of Fortune 500, category leading enterprises and trailblazing businesses. Access ACTIR's threat research taxonomy. Ready to see how the Arkose Account Security platform can protect your enterprise from threat actors and enhance your online fraud protection strategy? Schedule a call with an expert today.

METHODOLOGY

Our research methodology leverages Arkose Labs' unique position at the intersection of global digital commerce and security. Drawing on anonymized, aggregated data from our cross-industry customer base, which is composed of the world's biggest brands—we conducted a comprehensive analysis of scammer activities throughout Q1 and Q2, 2025. The study examined attack vectors, methodologies and behavioral patterns, with particular focus on in-quarter proportional trends, quarter-over-quarter trends and comparative metrics. We tracked the numbers of attacks and the size of attacks that scammers propagated, and we also mapped apparent geographical origins and target destinations, noting U.S. companies as primary targets. Temporal analysis identified peak attack periods based on local time zones in the countries studied.

Ready to see how the Arkose Account Security platform can protect your enterprise and enhance your fraud prevention strategy? Schedule a call with an expert today.

USA (San Mateo)

Australia (Brisbane)

United Kingdom (London)

Costa Rica (San José)

India (Pune)

Argentina (Buenos Aires)

TALK TO AN EXPERT