# SOCIAL MEDIA INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS

# 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% |

ATO attempts dropped quarter over quarter, consistent with broader industry patterns. The decline in average size indicates reduced intensity.

**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**

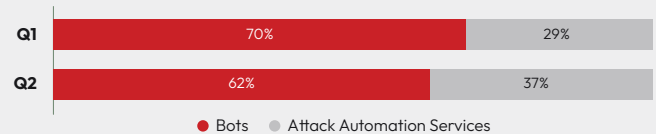
- **Attack automation services:** +1% attacks, -4% malicious traffic, -5% average attack size
- **Bots:** -29% attacks, -33% malicious traffic, -6% average attack size

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**




• Human fraud farms: +200% attacks, +412% malicious traffic*, +71% average attack size*

# 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.

## 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.

## CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When social media platforms implement adaptive security and deploy detection systems tuned for evolving threats, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, social media teams can move from reactive security to proactive defense—protecting not just user accounts and personal data, but the authentic human connections that make social networks meaningful.

## ABOUT ARKOSE LABS

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

**USA** (San Mateo)

**Australia** (Brisbane)

**United Kingdom** (London)

**Costa Rica** (San José)

**India** (Pune)

**Argentina** (Buenos Aires)

Book a Meeting