DATING INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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 vectors.

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.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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 31%
- 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.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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 62% 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

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When dating platforms implement adaptive security that scales friction with risk and deploy behavioral biometrics that distinguish humans from sophisticated automation, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, dating platform teams can move from reactive security to proactive defense—protecting not just accounts, but the authentic human connections that make online dating valuable.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM