# MEDIA INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS

# 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**

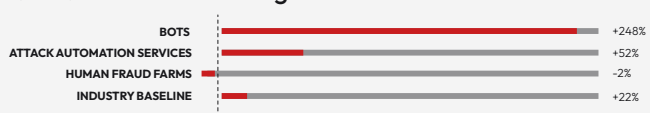
- **Attack automation services:** +21% attacks, +52% malicious traffic, +26% average attack size
- **Bots:** +78% attacks, +248% malicious traffic, +95% average attack size
- **Human fraud farms:** +200% attacks, -2% malicious traffic, -67% average attack size

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 Browser |

# 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.

## CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When streaming platforms implement session monitoring and anomaly detection for authenticated environments and deploy bot detection tuned for volumetric campaigns, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, streaming media teams can move from reactive security to proactive defense—protecting not just subscriptions and stored credentials, but the entertainment experiences that audiences value.

## 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