Enterprises Under Attack: Quarterly Threat Actor Patterns

Industry Trends, Analysis and Benchmarks | **Released Q4 2025**

ARKOSE LABS

TABLE OF CONTENTS

INTRODUCTION

As the winter holidays approach, it's still full steam ahead for our threat research team!

Cybercrime never stops, and fraudsters are continuing to refine their processes and bolster their toolkits. We've long known that taking down the bad guys is a marathon not a sprint. The data from the most recent quarter underscores the fact that scammers are constantly switching tactics and targets.

Last quarter, we reported that agentic AI and attack automation services are democratizing sophisticated cybercrime. The latest data reveals an important shift: Q3 shows a swing back to increased bot activity, potentially signaling that attackers are potentially beginning to deploy agentic AI for bot attacks at scale. This pattern is especially pronounced in retail and social media. While attack automation services declined this quarter, automation remains key for orchestrating sophisticated attacks at scale, suggesting this decline may be temporary.

In this comprehensive report, you'll find industry-agnostic trends revealing how fraudsters operate globally, deep dives into major industries, and intelligence to help you understand where your defenses stand relative to the broader threat landscape.

This isn't just data; it's your playbook for outsmarting fraudsters. These insights give you the intelligence needed to strengthen your defenses and ultimately make cybercrime unprofitable.

Every attack we stop, every scam we dismantle, and every fraudster we force to move on is a win for both our bottom line and the millions of consumers counting on us to keep them safe!

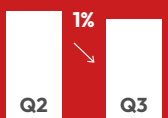
And as always, if you're staring down an urgent situation or have questions, just reach out to us directly.

Stay vigilant,

Frank Teruel
Chief Operating Officer
Arkose Labs

KEY FINDINGS

ATTACK VOLUME HOLDS STEADY



Q3 over Q2, attacks decreased by just 1%, while average attack size decreased 36%

FAKE ACCOUNT CREATION REMAINS THE LEADING ATTACK TYPE

comprising 46% of all attacks

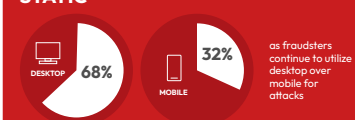
UTILIZATION OF HUMAN-BASED ATTACK SERVICES GREW

increasing by 24% Q3 over Q2

ATTACK AUTOMATION SERVICE FRAUD INCREASED IN AVERAGE ATTACK SIZE

Q3 attack volume decreased 16%, but average attack size increased 6% QoQ

DEVICE PATTERNS STAY MOSTLY STATIC



as fraudsters continue to utilize desktop over mobile for attacks

CONSOLIDATION TO CHROME CONTINUES

with 71% of all attacks coming from a Chrome browser

BRAZIL REMAINS A CYBERCRIME HOTSPOT

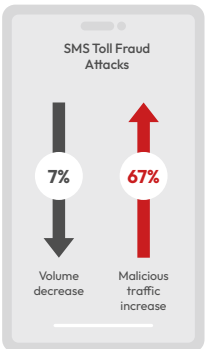
Excluding U.S. traffic (often masked), Brazil continues to lead as the country with the most attacks originating from it, followed by

ATTACK TYPES

As in other quarters, the leading attack type in Q3 2025 was fake account creation, accounting for 46% of attacks. This ongoing trend demonstrates that securing sign-up flows should be a prime concern for businesses, particularly if they offer online products and services with loyalty points or other bonuses that scammers may seek to exploit.

Account takeover held steady as the second most popular attack type, at 29% of all attacks. Payment-based attacks also saw an uptick with strong Q3 over Q2 growth (50%) suggesting that fraudsters remain adept at scaling fast once they hit upon a new successful attack strategy.

After growth in Q2, MFA compromise dipped in Q3, both in terms of attack volume and malicious traffic. Meanwhile, SMS toll fraud attack volume declined as malicious traffic associated with this attack type ballooned 67% QoQ, suggesting that fraudsters are refining their SMS attacks, choosing targets carefully and increasing the scope of each attack.



ATTACK MECHANISMS

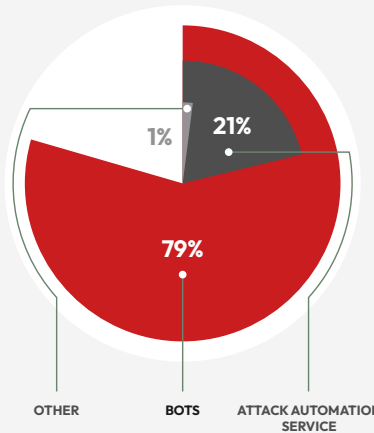
Volumetric attacks continue to dominate the fraud landscape, with bots accounting for more than two-thirds of all attacks in Q3. Attacks originating from human fraud farms grew by 24%, while attacks from attack automation services shrank by 16%.

Insights into threat actor behavior show that automation is key for orchestrating sophisticated attacks at scale, so the decline of attack automation services might be an anomaly for this quarter. We'll continue to monitor this as our research shows there are likely to be more automated attacks using agentic AI that adapt and learn, supercharging scammer operations and changing the economics of these attacks.

The Q3 attack mechanism spread shows that bot attacks are still the bread and butter for fraudsters. Cheap and easy to execute, this attack mechanism typically has low success rates but is highly scalable, making volumetric attacks using bots profitable for even inexperienced fraudsters.

With this solid basis in place, other attack mechanisms can be trialed and switched. Our quarterly data shows that attack automation services and human fraud services like fraud farms continue to be used by scammers. The average attack size of scams deploying attack automation services increased by 6% quarter over quarter, suggesting that fraudsters are scaling and refining their attacks to get more mileage out of each. And while human-orchestrated attacks still account for less than 2% of all attacks, the surge in attack volume and malicious traffic from operations such as fraud farms in Q3 shows that these low and slow attacks are still on cybercriminals' radars.

MALICIOUS TRAFFIC BY ATTACK MECHANISMS IN Q3



Note: Numbers don't add to 100% due to rounding

ATTACK DEVICES, BROWSERS AND COUNTRIES

Mobile vs Desktop Split

Once again, desktop remained dominant, with 68% of attacks orchestrated this way versus 32% via mobile.

TOP 5 BROWSERS BY NUMBER OF ATTACKS, Q3 2025

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

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

The U.S. led attack origins, but since fraudsters frequently spoof U.S. locations to appear as legitimate domestic traffic, we exclude this data when ranking countries by attack volume.

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

ATTACK TIMING

Scammer Daily Activity Patterns, by Country

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.

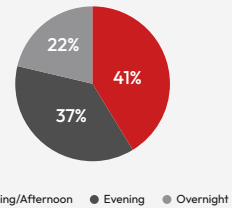
- Morning/Afternoon: 8 a.m. - 4 p.m. Local Time
- Evening/Night: 4 p.m. - 12 a.m. Local Time
- Late Night/Early Morning: 12 a.m. - 8 a.m. Local Time

In Q3, we saw slight consolidation toward both daytime and evening attacks, with strikingly similar numbers for each, while overnight attacks declined.

When attacks appear to originate from the U.S., many of these are global attacks using location spoofing. In Q2, 50% of such attacks came during the daytime within typical business hours, while in Q3, 47% of attacks appearing to be from the U.S. came during the same window.

As in Q2, 48% of Great Britain's attack traffic was concentrated to evening hours in Q3.

Attack timestamps for Brazil, Q3's leading country for originating attacks.



In the Philippines and Pakistan, patterns held steady against Q2, with Q3 attack traffic clustering in the evening for these regions. India also had a high volume of attack traffic occurring late in the day, with the evening timestamp accounting for 42% of traffic.

Last quarter, we observed that countries that have strong fraudulent traffic throughout a full 24-hour day could be hotbeds for cybercrime rings, with professional operations and round-the-clock shifts to orchestrate both volumetric and human-driven attacks. This pattern can be seen in both Mexico and Vietnam, which have remarkably similar attack traffic volumes across all three timestamps.

RECOMMENDED ACTIONS

Address the Reality of Agentic AI

The advent of widespread use of agents by consumers and fraudsters alike is making good and bad users even more difficult to tell apart. Traditional detection methods that rely on identifying automation patterns are growing less effective. Companies must adopt intent-based analysis and contextual risk scoring to distinguish between legitimate AI-assisted users and malicious agents.

Deploy Device Identification

Fraud continues to consolidate to Chrome browsers, hiding in plain sight and exploiting the extension ecosystem. This shift of cybercrime to popular consumer browsers further underscores the need for careful device fingerprinting, to identify emulators and device farms before they do damage.

Balance UX With Security

Companies should devise a strategy to carefully balance experience for good users with strong and robust security. By breaking down silos between internal teams, while bolstering continuous authentication and anomaly detection, security leaders can prioritize a delightful user experience without making compromises that open their platforms to additional misuse.

Continue to Secure Sign-In and Sign-Up

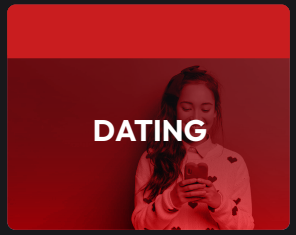
Most attackers still use account creation and account takeover to scam companies. Consider implementing behavioral biometrics to distinguish humans from automation services, and use passwordless solutions resistant to credential stuffing.

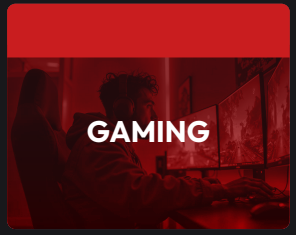
Fight Automation With Automation

Fraudsters are refining their use of attack automation services, orchestrating larger scale attacks which threaten to have devastating consequences for companies. Security teams should remain vigilant, screening for large volumes of unusual traffic to stamp out these mass attacks, and using solutions designed to screen for these increasingly sophisticated volumetric attacks.

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

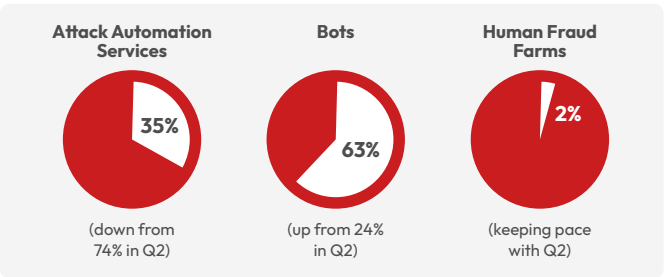
As in Q2, a majority of the attacks on dating platforms during Q3 started at sign-in.

Account Takeover (ATO): Expanded and Intensified	Attacks: +208%

ATO remained the dominant threat for dating platforms, with substantial growth in malicious traffic and attack size.

While attack automation services dominated the dating industry attack landscape in Q2, bots were back with force in Q3, accounting for 63% of attack volume and 86% of malicious traffic.

Attack Mechanism Distribution by Number of Attacks



While adoption of attack automation services previously suggested that fraudsters were investing in specialized toolkits designed specifically for dating platform attacks, the surge for bots hints that scammers may have a new tactic: deploying agentic AI. They may have used recent months to train their own bots on attack automation service models, supercharging their abilities to launch romance scams at scale. As we examine more data, we'll be able to analyze whether this decline is an anomaly or part of a broader shift as fraudsters transition to agentic AI that adapts and learns.

In Q3, Chrome continued to dominate, with Chrome, Chrome Webform and Chrome Mobile being the most popular browsers. Mobile Safari was the next most used by attackers.

The shift to mobile from desktop that was observed in Q2 held steady, with 60% of attacks coming via mobile devices.

For dating industry companies, the countries with the most attacks originating from them are India, Indonesia and Brazil.

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

	India
	Indonesia
	Brazil
	Morocco
	Great Britain

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

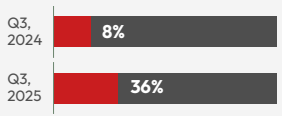
FINTECH INDUSTRY ATTACK LANDSCAPE

The fintech industry saw dips in attacks in Q3 2025, versus the prior quarter, with attacks falling by 73% overall. Despite this overall reduction, SMS toll fraud ballooned, with attack volume increasing 11%, and malicious traffic by 97%. It's a sign that revenue sharing fraud remains a major attack vector, and the major growth in the average attack size demonstrates that criminals are honing their ability to scale once they identify a vulnerable flow that they can exploit for financial gain.

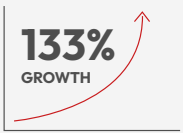
11% increase
in SMS toll fraud

The downwards shifts for most attack types including account takeover, fake account creation and in-app threats suggests that some fintech firms have been successfully bolstering their defenses against attackers, securing login and sign-up flows to disrupt the economic payoff of attacks against this sector. Time is money for bad actors, so when companies prove time-consuming to infiltrate, many scammers will move on.

Despite overall attack declines, attacks orchestrated by human fraud farms grew in this industry by 133% in Q3. This suggests a gearshift by scammers, who might be abandoning a volumetric scattergun approach to fraud against fintech companies, in favor of smaller scale highly targeted attacks.



YoY comparison, attack automation service share of attacks



in human-orchestrated attacks QoQ

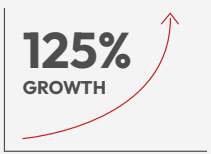
Chrome maintains dominance for scammers targeting fintech companies in Q3, and the shift towards mobile continued, bringing the two device types roughly neck and neck.

Attack geography data reveals that the most popular country for launching fintech attacks in Q3 was Pakistan.

GAMING INDUSTRY ATTACK LANDSCAPE

As in Q2, fake account creation is the dominant attack type in the gaming industry. Expanding in-game economies and payment integrations have made transactional endpoints especially lucrative for attackers seeking quick monetization. Payment-based attacks declined QoQ, while SMS toll fraud grew 125%.

These patterns show shifts in fraudster strategies, not that fraud against gaming companies is slowing down. Attack volume shifted by less than a percentage point between Q2 and Q3, while malicious traffic grew 8% and average attack size grew 9%. Bot attacks accounted for 73% of all attack traffic.

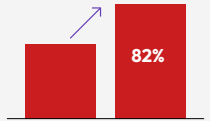


SMS toll fraud

Versus Q2 this year, we saw attack automation services decrease in volume, yet the 73% increase in malicious traffic shows that these attacks are ballooning in size. The average attack size for human-orchestrated attacks against the gaming sector decreased 94%, while attack automation service average attack size increased 82%. This attack automation service volume decline might be an anomaly, or an early indicator of a new normal as fraudsters adopt agentic AI.

In Q3, browser consolidation toward Chrome continued. While use of gaming-specific browsers by scammers previously suggested exploitation of embedded browsers to blend with legitimate player traffic, the recent shift hints that bad actors are encountering less friction with mainstream browsers. More than half of bad actor traffic came from a Chrome browser.

Desktop remains the favorite device type within gaming: 81% of traffic came via desktop, up from 70% via desktop in Q2. The distribution of the top countries from which attacks on gaming platforms originated also held steady, with Brazil, the U.K. and Vietnam comprising the top three once again.

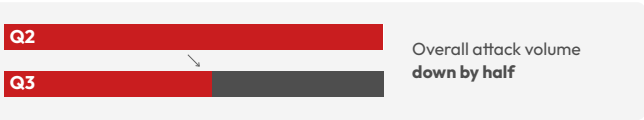


Attack size of attack automation services attacks increased 82%

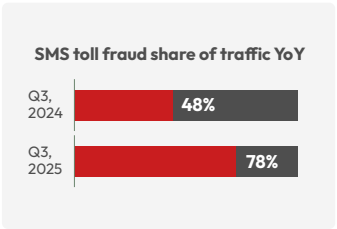
of attack traffic came via desktop

GIG ECONOMY INDUSTRY ATTACK LANDSCAPE

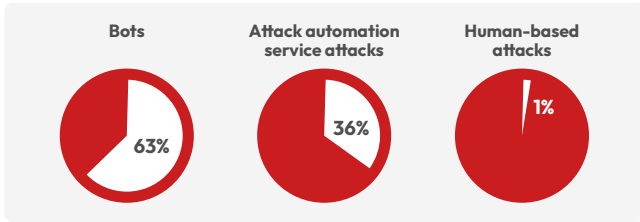
Compared with Q2, scams against the gig economy sector were smaller in number but larger in size. The Q3 attack volume was down by 51%, but malicious traffic was up by 49%, and average attack size increased threefold. This pattern shows that fraudsters are honing the attacks and putting their energy where it pays off the most, focusing on fewer attacks with larger scales.



Account takeover and SMS toll fraud were the attack types where these patterns were seen most starkly. SMS toll fraud accounted for 78% of all Q3 2025 attacks observed against the gig economy sector, compared with 48% in the same quarter in 2024.



The shift away from the MFA compromise focus seen in Q2 underscores the constantly changing tactics of fraudsters, who are ready to pivot once companies become adept at shutting down their schemes. Despite the attack type shifting, the mechanism did not, with the spread of bot attacks and scams orchestrated by attack automation services matching the patterns seen in Q2.

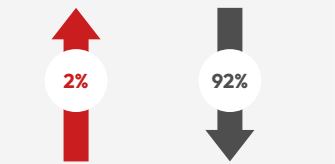


In terms of device and browser preferences of fraudsters operating against the gig economy sector, there was little movement, with mobile gaining a slightly larger share of attack traffic. Chrome variants continued to dominate browser distribution.

As in Q2, Brazil continued to be a top country for originating attacks, followed by India, Canada, Pakistan and Great Britain.

MEDIA INDUSTRY ATTACK LANDSCAPE

Media and streaming platforms were one of few industries to see a small increase in attacks quarter over quarter, contrasting with the decline seen across industries overall. The dominance of account takeover attacks grew to 85%. Despite attack volume increasing, malicious traffic plummeted by 92% QoQ. This dramatic shift in attack scope could mean that attackers are switching some of their focus to other markets, possibly in response to free trials or promotion cycles.



of media industry attacks are account takeover

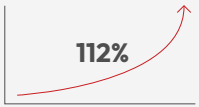
Bot attacks accounted for 68% of the attacks orchestrated against media and streaming platforms in Q3, up from 53% in Q2. It's an increase that might be partially driven by fraudsters increasingly experimenting with agentic AI. Meanwhile, the number of human-driven attacks fell by a third, yet malicious traffic from this attack type skyrocketed by 1048%. While these attacks, which likely originate from fraud farms, still account for less than 2% of scams in this market segment, companies should keep an eye on this increasing scope.

Chrome remained the most popular browser, and desktop dominance also stayed static. In terms of country distribution, all three top countries changed versus Q2, with France, Great Britain, and Poland leading attacks against this sector during Q3.

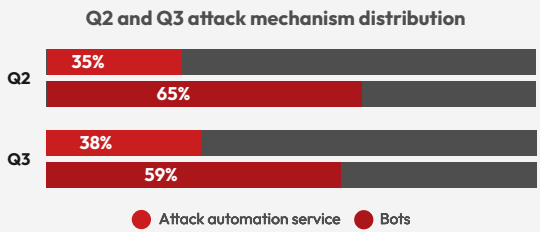
Media Industry: Top 3 Attack Origins (Excluding U.S.)
France
Great Britain
Poland

RETAIL INDUSTRY ATTACK LANDSCAPE

Fake account creation continued to plague retailers in Q3 as in Q2, with a 112% increase in attack volume, and a fivefold increase in malicious traffic. Even as attacks rocketed, attack mechanism distribution remained fairly static, with a small QoQ shift toward attack automation service.



QoQ increase in fake account creation attack volume



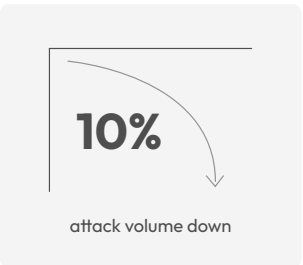
This broad preference for bots by attackers targeting the retail industry in recent quarters chimes with patterns observed in Q3 2024, when bots accounted for 79% of attacks.

Mobile's share of traffic was substantial, bucking the trend of a preference for desktop in other industries and demonstrating that fraudsters are hiding in plain sight, attempting to blend in with legitimate traffic given the growing prevalence of the mobile experience in retail. Mobile Safari was the most popular browser.

Attacks originating from India dominated the spread of geographically traceable traffic.

SOCIAL MEDIA INDUSTRY ATTACK LANDSCAPE

Social media platforms saw declines in fraud quarter over quarter. Attack volume dipped 10%, and malicious traffic plummeted by 85%. This shift suggests the social platforms have found ways to bolster authentication and mitigate the in-app threats that plagued them in Q2.



More than three quarters of attacks were via fake account creation. The spread of attack mechanisms changed, shifting 11 percentage points from attack automation services toward bots. This could be an anomaly, a hint that fraudsters are becoming more adept at training their own bots based on these previously utilized services, or a signal that fraudsters are shifting to bot-heavy attacks due to the use of adversarial agentic AI tools.

The desktop/mobile split held steady, with 73% of attacks still coming from desktop devices in Q3. Browser fingerprinting shows that Chrome dominates the desktop-based traffic (83%), with smaller volumes coming from Firefox (6%) and Microsoft Edge (4%).

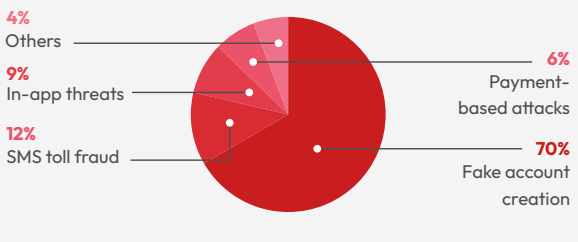
Social Media Industry: Top 3 Attack Origins (Excluding U.S.)	
	Vietnam
	Brazil
	Turkey

Compared with Q3 2024, social media attacks are down by more than a third. And this year, there's a stronger concentration of attacks at registration, with 76% of fraud starting at fake account creation versus 70% in the same period last year. These swings suggest both prioritization and consolidation: it's possible that fraudsters are keeping some of their tried and tested attack tactics on a simmer while tooling for attacks in other markets.

TECHNOLOGY INDUSTRY ATTACK LANDSCAPE

In the technology space, attacks decreased 7% QoQ. Fraudsters are continuing to use attack automation services: while this attack mechanism accounted for 31% of attacks in Q2, this segment was up to 38% in Q3. Looking back to Q3 of 2024, attack automation services were at 41% of all attacks. This clustering over time shows that we can expect around a third of all attacks against the tech sector to deploy CaaS products.

Meanwhile, bot traffic declined 18%, and the average attack size of bot attacks more than halved. This could hint that fraudsters are winding down their broad campaigns targeting tech companies with volumetric attacks, and tooling for smaller volumes of more bespoke attacks. And while fake account creation dominated in Q2, making up 88% of attacks, this attack type was down to 70% this quarter, with in-app threats and SMS toll fraud both showing growth.



Note: Numbers don't add to 100% due to rounding.

As in Q2, browser fingerprinting in the technology sector reveals a high concentration of Chrome use, with this browser being utilized in 80% of desktop attacks.

Technology Industry: Top 3 Attack Origins (Excluding U.S.)	
	Russia
	India
	China

CONCLUSION

The combination of lower attack volume along with larger attack sizes observed in Q3 demonstrates that fraudsters are inclined to go all-in when they discover an easy-to-exploit entry point. These large attacks with substantial malicious traffic can cause havoc in short timeframes for companies affected, flooding platforms with fraud and eroding the experience for good users. When attacks come in smaller numbers but with full force, every single fraud mitigation counts.

We know that fraudsters are beginning to deploy agentic AI powered attacks, and growing bot dominance supports this. The shifts we see over time in terms of attack types and mechanisms shows that fraudsters are constantly retooling and refining their strategies. But they can be beat. The declines in attack volumes observed in some sectors strongly suggests that fraudsters are walking away from scamming angles that cost them too much time and money.

Making cybercrime unprofitable should remain a prime objective for companies. And as consumers increasingly use agents for their online transactions, telling good agent traffic apart from adversarial agentic AI will be the next frontier in this ongoing battle. Armed with strong data and advanced tools, you can continue to protect your customers from fraud in this new digital era.

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 Q2 and Q3, 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.

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)

TALK TO AN EXPERT