WHITEPAPER

# A DATA-DRIVEN ANALYSIS OF THREAT ACTOR BEHAVIOR

## Uncovering Where Scammers Focus Their Efforts and Their Tactics of Choice

# A DATA-DRIVEN ANALYSIS OF THREAT ACTOR BEHAVIOR

## Table of Contents

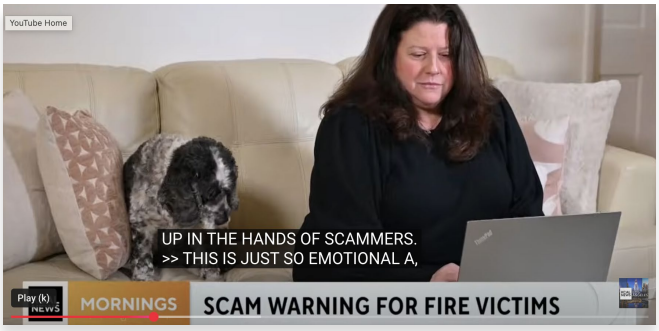
# INTRODUCTION

To defeat your adversaries, get inside their mind. Simple as that. That's why we've analyzed a full year of cross-industry data from the biggest, most targeted enterprises in the world. And let me tell you, the results are eye-popping. We're in a scamdemic!

Here's the twist: What starts as bonus abuse or loyalty point theft quickly metastasizes into far worse crimes—terrorist financing, human trafficking and those sophisticated "pig butchering" schemes. When left unchecked, they bleed into money laundering operations, carrying substantial regulatory fines whether you're working in cybersecurity, anti-fraud at a bank or any other industry. There's no arguing with the ballooning scope of scams. The FBI recently released its Internet Crime Complaint Center (IC3) report for 2024. It revealed that last year saw a new record for losses reported, and more than $3 billion was due to account-based attacks.

Today's scammers? Bold doesn't begin to cover it. "No, no remorse," a scammer named Mayowa confessed to USA Today when asked about stealing from Americans. "We don't know them...it's nobody."[1] Chilling, right? This candor reveals a fundamental truth: Fraud is a career, plain and simple. A single bad actor can pocket US$145,176 targeting just five premium gaming platforms with account takeover scams (**see page 26**). Scale that across hundreds of sites, and it becomes a massive money-maker, regardless of geo.

While enterprises face significant risks, consumers bear the brunt. Just recently, Angelino Kim Chase told CBS News how identity theft delayed her critical FEMA wildfire relief funds when she needed them most.[2]




Stopping these attacks isn't just good business. It's a humanitarian effort! This report pulls back the curtain on the strategies and behaviors these scammers deploy daily. We're zeroing in on those critical choke points where bad actors either get stopped cold or break through so that you can secure your company and strengthen consumer protection by understanding your enemy a little bit better.

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

Sincerely,

**Frank Teruel**
Chief Operating Officer
Arkose Labs
f.teruel@arkoselabs.com

[1] https://www.usatoday.com/in-depth/news/investigations/2020/12/30/unemployment-fraud-how-international-scammers-took-36-b-us/3960263001/
[2] https://www.youtube.com/watch?v=lHLp6D9RHil

# EXECUTIVE SUMMARY

Why do scammers scam? Scammers operate with a three-part mindset: motive, opportunity and rationalization. Money drives them, opportunity abounds through dark web tools and AI capabilities, and they justify attacks as necessary income. Enterprises cannot eliminate financial motivation or personal justifications, but they can remove opportunity. Advanced security solutions target this vulnerability by increasing intrusion costs, making attacks economically unfeasible. By destroying opportunity through prohibitive costs, these defenses break the scammer's essential framework, preventing even motivated criminals from profiting.

The scammer profit motivation creates exploitable patterns. Our analysis of nearly 20 billion malicious attack traffic patterns for this report reveals that scammers abandon targets when ROI drops below certain thresholds. A few fundamental truths exist: When the cost to attack is more than the gain, scammers quickly pivot to weaker targets.

Understanding this mentality is the first step in stopping your adversaries. A second truism: Attackers are incredibly agile and unconstrained by the policies and practices that often restrict enterprises from quickly adopting technology even when that adoption will mitigate adversarial behavior. A third truism: Scammers perfect attacks across industries and then share their exploits, sources and methods, and resulting financial gains with great alacrity.

By understanding attack entry points, attack types, time-of-day attack rhythms and other patterns, security leaders can begin to predict and preempt behavior to strategically disrupt scammer economics. Exploiting scammers' relentless pursuit of favorable cost-to-attack ratios forces them to abandon targets when profitability evaporates.

This report provides actionable intelligence to help you understand the adversary so that you can use their force and momentum against them.

Our threat researchers have seen clear "testing progression" behavior by scammers. Rob Morera, security operations manager on the Arkose Labs SOC team, explained it this way:

“We've observed a concerning pattern where attackers methodically develop and test their tools against various sectors, like gaming or gig economy, often documenting their techniques in public GitHub repositories and leveraging machine learning and AI. Once these methods prove effective, more sophisticated threat actors with greater resources adapt these techniques and redirect their focus specifically toward financial institutions. Ultimately, financial organizations find themselves defending against complex, hybrid attack methodologies from adversaries united by a single objective: committing fraud.”

## 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

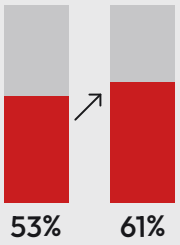
**$1.03 TRILLION WAS LOST TO SCAMS GLOBALLY IN 2024[3]**

### VULNERABLE ENTRY POINTS


of scams started through account sign-up flows

### EVOLVING ATTACK TYPES

Fake account creation surged from




SMS toll fraud more than doubled to 9%

### WEAPONIZED ATTACK MECHANISMS

Categories

**2,046%** Q2oQ1 ↑
Relentless Attack Automation Services

**957%** Q2oQ1 ↑
Coordinated Fraud Farms

**556%** Q4oQ3 ↑
Shape-Shifting Advanced Bots

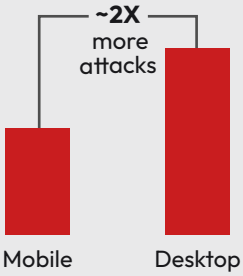
**173%** Q4oQ3 ↑
Bots

### SCAMMER SALARY


Scammers in El Salvador might make **20x** more attacking gaming companies, versus working a software developer job

### POPULAR ATTACK DEVICES

ACCOUNT TAKEOVERS




### ATTACK TIMING TRENDS

ACCOUNT TAKEOVERS

**60%**

of attacks originating in El Salvador occur between **4 p.m. to 12 a.m.** Local Time (Central Standard Time)

### SCAMMERS TOOK A BREATHER

Among the target industries in this report, August and September malicious traffic accounted for less than 1% of all annual malicious traffic

[3] https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

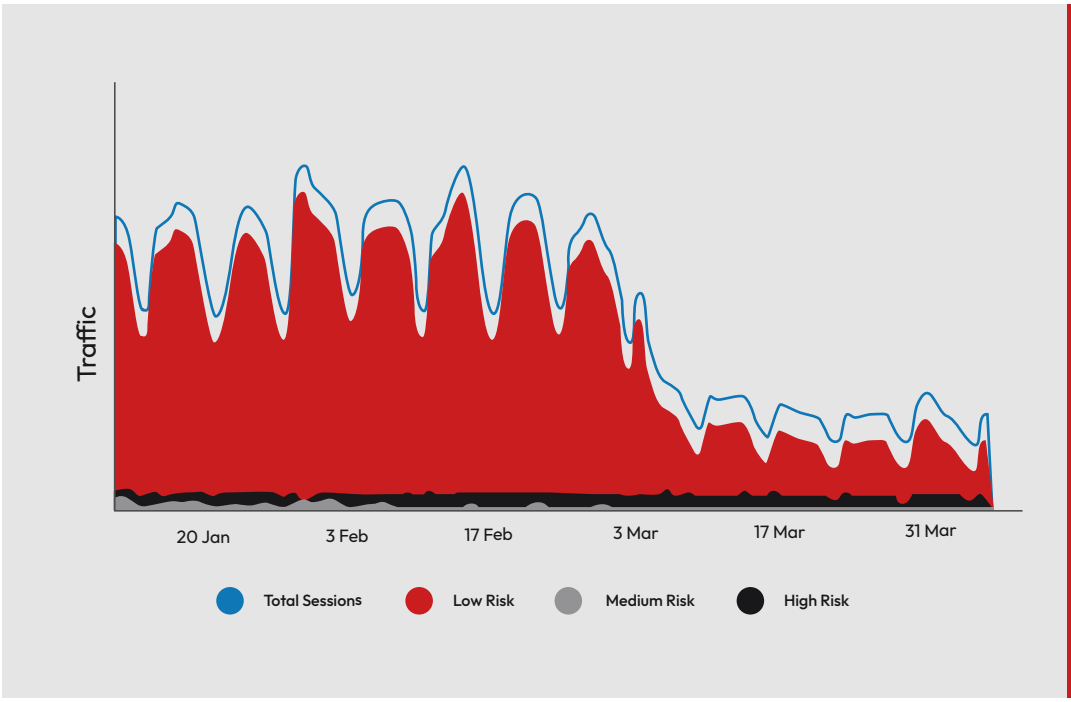
# BUT FIRST THE GOOD NEWS

Despite relentless scammers, the good news is that companies and their customers are proving equally persistent. Microsoft alone processes over 78 trillion security signals daily through its cloud, endpoints and partner ecosystem to protect against digital threats.[4] In 2024, Arkose Labs protected billions of legitimate transactions, ensuring consumers enjoy seamless and safe digital experiences.

In recent examples, one company reported 98% of its traffic came from legitimate customers, directly impacting satisfaction, loyalty and revenue. Conversely, overly aggressive online fraud prevention measures that interfere with legitimate users can cost companies millions in lost revenue and damaged relationships.

The real value proposition isn't just stopping bad actors—it's ensuring that good customers sail through authentication and verification processes without unnecessary friction, leading to profitable growth.

But what we truly know and experience every day is that threat actors do attempt to hide in this legitimate traffic. We expose their tactics and behaviors throughout the remainder of this analysis, starting with one of the most profitable and widespread attack vectors targeting B2C platforms today: ticket botting.




**98%**

of good users have seamless experiences

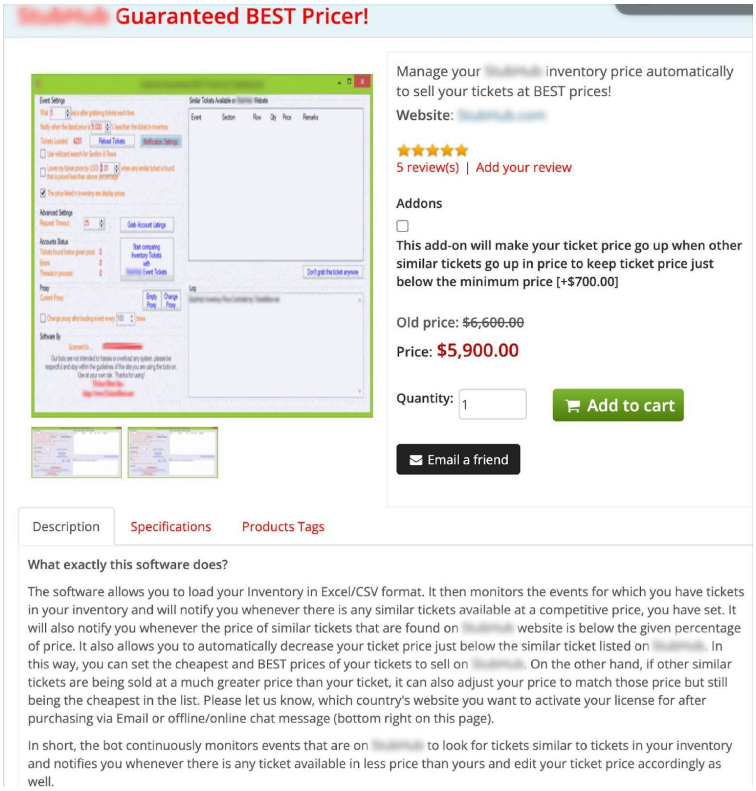
[4] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

# THE TRUTH ABOUT TICKET BOTTING

Ticket bots have evolved into a sophisticated criminal ecosystem with three distinct tiers. Commercial bot vendors charge up to $550 annually for tools targeting major platforms like Ticketmaster, SeatGeek, StubHub, etc; dark web marketplaces peddle fake ticket generators and pre-loaded accounts with payment methods attached; and Telegram networks extract $50-$150 per event from members while sharing cookie tactics to unlock reserved seats—often scamming their own participants, emphasizing there is no honor among thieves.

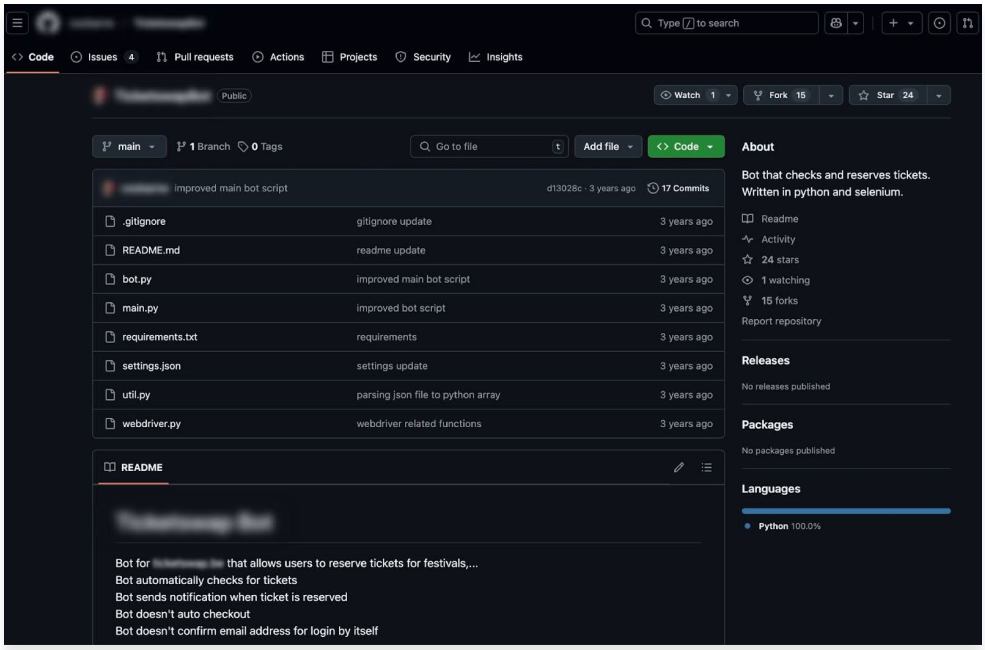
The latest techniques go beyond simple automation. Scammers now exploit "Buy Now, Pay Later" services using hijacked accounts, deploy $6,000 algorithmic programs to maximize profits on resale platforms and coordinate networks of fake accounts to bypass purchase limits.

The threat, though, expands beyond entertainment to airline systems, where specialized bots pounce on fare drops and flash promotions. These programs stalk pricing errors and discount opportunities, with travel tickets becoming particularly valuable during high-demand periods. Unlike the sneaker market where manufacturers eventually crushed bot networks, ticket botting entrenches itself as a persistent, evolving threat that simply pivots to new territories when countermeasures emerge in one sector.



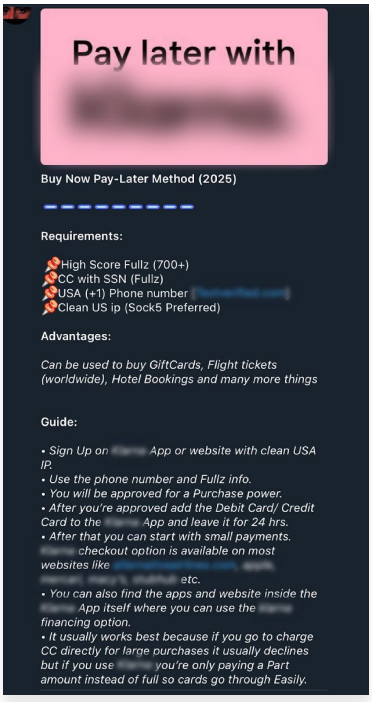

**ABOVE:** A screenshot of a dynamic pricing algorithm bot designed for ticket resale markets.

This specialized software—which can cost up to US$6,000—automatically monitors and adjusts ticket prices on secondary platforms, ensuring scalpers maximize profits by responding to real-time demand fluctuations. Attackers can also manipulate markets by “flooding” tickets at considerably lower prices to recoup funds if the secondary market for an event is weak, almost permanently reducing the value of tickets, which can impact the event organizers and marketplace. Such sophisticated tools represent the evolution of ticket botting beyond basic purchasing automation into advanced market manipulation techniques that target the entire lifecycle of ticket sales.




**ABOVE:** A screenshot of a bot freely available on a collaborative workspace that is used for software development

This bot automatically checks for tickets and reserves them for checkout by a consumer. The scammer will receive a notification when ticket(s) are reserved and they (the scammer) can check out. The bot's design deliberately requires manual completion of checkout and login processes, potentially allowing scammers who use it to circumvent laws (such as those in Australia) that specifically prohibit fully automated ticket purchasing.




**ABOVE:** A screenshot showing the "Buy Now, Pay Later" exploitation scheme that has become prevalent in ticket scams.

Fraudsters use compromised accounts or create fake new accounts with stolen personal information to purchase tickets through BNPL services, then quickly sell these tickets on secondary markets. By the time the fraud is detected, purchases are voided, and refunds are made to consumers—often weeks later—scammers have already made their money. This timing gap creates a profitable window for cybercriminals.

# SCAMMER ATTACK PATTERNS

**Most Attacked Industries with the Biggest Attacks**

Scammers target industries that offer the greatest financial return or valuable credentials that enable further profitable attacks. The ranking below shows attack scale and size rather than volume, showcasing where scammers invest their most significant attempts. We highlight meaningful industry-specific, data-driven insights in each section of this report. The data clearly shows scammers aimed at social media companies throughout the year, but hyper-targeted them around the U.S. presidential election (see Graph 1 on page 19).


# ATTACK POINTS: WHERE SCAMS BEGIN

Scammers target vulnerabilities at the intersection of low security and high value across consumer accounts. Analysis reveals three critical vulnerability points:

## Account sign-up (most common entry point)

Account sign-up remains scammers' preferred entry point, offering maximum return with minimal effort. Their timing strategy is calculated: testing defenses during political events mid-year, then launching their heaviest attacks during the holidays when security teams are stretched thin and high legitimate traffic provides perfect cover.

- Scams starting at account sign-up consistently accounted for over 50% of all attacks throughout 2024.
- Proportionally, nearly two-thirds of all attacks in Q4 began at sign-up.
- The growth in sign-up attacks peaked in Q3, with a 48% increase over Q2 (likely due to the U.S. election).
- The largest sign-up scams as measured by malicious traffic occurred during the Q4 holiday season (309% over Q3).

**11,600% ↑ Q3◦Q2**

**Fintech:** The number of attacks at sign-up surged 11,600% in Q3 compared with Q2. Most attacks involved SMS toll fraud (AKA international revenue share fraud). Scammers likely used increased online activity during the Paris Olympics to mask these "grab and go" scams involving telcos. An ACTIR[5] unit threat researcher notes, "There is no profit incentive for the scammer without telco collusion."

**4,900% ↑ Q4◦Q3**

**Dating:** These platforms saw a 4,900% surge in the number of sign-up attacks during Q4 compared to Q3 as scammers exploited the holiday season to launch romance scams. Scammers created fake accounts throughout Q4 and laid the groundwork for human

[5] Arkose Cyber Threat Intelligence Research unit

trafficking. The most recent Polaris[6] report notes that on the Internet, dating sites are the top recruitment location for human trafficking, which is a predicate offense to money laundering. A global dating platform lost significant customer trust when scammers exploited minimal sign-up requirements to flood the platform with fake profiles and entice legitimate users to click malicious links, ask for money or engage in phishing schemes. Deploying advanced behavioral analytics finally thwarted these attacks.[7]

**1,047%↑ Q2oQ1**

**Media:** The dramatic surge in streaming media attacks during Q2 2024 saw attack numbers double while size exploded by 1,047% compared to Q1. This period featured season finales and blockbuster premieres that masked fraudulent activity amid legitimate subscriber growth. Additionally, the northern hemisphere's transition to summer vacation increased leisure viewing, especially among younger users finishing school years, which may have driven demand for illicit streaming access. Scammers expertly timed their campaigns to exploit this perfect storm of seasonal factors.

## Account sign-in

Authentication flows become prime targets when account takeovers or phishing can succeed, providing access to consumer accounts from which scammers can drain funds or exploit valuable payment information. Companies must balance security with consumer experience at sign-in flows, creating an inherent tension that scammers exploit through social engineering, credential stuffing and identity spoofing techniques.

- Sign-in attacks peaked in Q2 at 29% of all attacks, then steadily declined to a year low of 19% in Q4.
- The first half of the year saw significantly higher attacks at sign-in as a proportion of all attacks (53% of annual total) than the second half (44%).
- A 10-point drop from Q2 to Q4 suggests scammers either faced improved security or shifted to more profitable attack vectors.
- The Q4 decline coincides with the reported surge in sign-up attacks, indicating scammers likely redirected their focus.

**1,342%↑ Q3oQ2**

**Media:** Scammers spent a significant amount of energy deploying attacks at sign-in aimed at the streaming media industry in early 2024, comprising 80% (Q1) and 85% (Q2) of all media industry attacks before dramatically dropping to 52% in Q3, then ticking up to 67% in Q4. Despite this proportional decline, Q3 actually saw a 35% surge in number of attacks and a 1,342% increase in malicious traffic (reflecting attack size) both compared to Q2. This pattern reveals two key insights: First, scammers strategically timed their most aggressive campaigns to coincide with the Paris Olympics, when heightened legitimate traffic provided perfect cover for scams at unprecedented scale. Second, while sign-in attacks represented a smaller percentage of Q3's total attack landscape for media companies, they grew significantly more sophisticated and concentrated—suggesting fraudsters were executing highly targeted campaigns to harvest and monetize streaming credentials when global demand for access to Olympic content peaked on dark web marketplaces.

[6] https://polarisproject.org/wp-content/uploads/2020/07/Polaris-Analysis-of-2021-Data-from-the-National-Human-Trafficking-Hotline.pdf
[7] https://www.arkoselabs.com/resource/online-dating-platform-ghosts-fraudsters-arkose-labs-aws-case-study

**2,242%↑ Q4oQ3**

**Dating:** Dating platforms experienced a paradoxical attack pattern in 2024. While attacks at sign-in plummeted from 100% of all attacks in Q1 to just 16% by Q4, the attacks at sign-in actually grew exponentially in intensity. Malicious traffic, which is a measure of scam size, surged 4,568% from Q1 to Q2, grew another 75% in Q3, then exploded by 2,242% in Q4. Similarly, the number of attacks dropped 33% in Q2 before increasing 100% in Q3 and skyrocketing 775% in Q4.

This contradiction reveals a sophisticated strategy: Scammers diversified their attack vectors while simultaneously concentrating resources on fewer, more devastating sign-in campaigns using account takeovers. The Q4 surge coincided with the holiday season, when scammers deliberately intensified efforts targeting emotionally vulnerable users. People seeking connection during holidays may be more willing to overlook warning signs or respond to suspicious messages, creating perfect opportunities for romance scams. This seasonal targeting demonstrates scammers' tactical evolution, combining technical sophistication with psychological manipulation for maximum impact.

## Account management

Scammers exploit human vulnerabilities through social engineering tactics that bypass technical security measures. When technical approaches are blocked, they pivot to support channels like call centers—a strategy particularly evident during the Paris Olympics time period.

- Proportionally, scams starting at account management declined steadily, dropping by more than half from Q1 to Q4.
- Q4's significant drop suggests improved holiday security protocols or more experienced seasonal staff in call centers.
- Companies likely strengthened call center security, pushing attackers toward other entry points, like account sign-in.
- Scammers spent time, energy and effort attacking account management throughout the year. But the number of attacks declined in Q2 and Q4 and slightly increased in Q3. Interestingly, though, attack size as measured by malicious traffic grew steadily for the first nine months of the year, with the most dramatic jump of 490% in Q3 over Q2.

**3,084%↑ Q3oQ2**

**Gaming:** While attack numbers at account management flows steadily decreased, Q3 saw a 3,084% surge in malicious traffic compared to Q2. This indicates sophisticated threat actors moved from widespread campaigns to concentrated "big game hunting" strategies, likely targeting high-value accounts during seasonal gaming releases and tournaments or exploiting specific vulnerabilities. The contrast between declining frequency and escalating size suggests scammers consolidated resources for maximum impact, possibly testing new methodologies. The subsequent drop-off after Q3 hints that gaming platforms strengthened defenses following this unprecedented spike, making account management a less attractive flow to target.While not one of the top 3 attack points across all industries, it’s interesting to note that attackers then pivoted to gaming industry payment systems, as evidenced by a staggering 45,854% increase (Q4 over Q3) in malicious traffic at payment flows. We believe this was caused by the holiday shopping season.

| | Quarter 1 | Quarter 2 | Quarter 3 | Quarter 4 |
|---|---|---|---|---|
| Sign-up | 55% | 50% | 60% | 64% |
| Sign-in | 24% | 29% | 25% | 19% |
| Account management | 16% | 14% | 12% | 7% |

**Table 1: Quarterly Breakdown: Where Scammers Focused Their Efforts** Table shows percentage distribution of attacks by the top 3 points of attack (sign-up, sign-in, account management) for each quarter. Read columns vertically to track scammers' quarterly priorities.

Analyzing attack points by malicious traffic (attack size) reveals scammers adapt rapidly, shifting between attack points, with sign-up showing sustained popularity while SMS exhibits volatility. An analysis reveals opportunistic patterns reflecting changing security landscapes or seasonal factors. The significant decreases in attacks at account management and sign-in during Q4 coincide with increased focus on sign-up and SMS, suggesting strategic resource reallocation by scammers.

| | Q2oQ1 | Q3oQ2 | Q4oQ3 |
|---|---|---|---|
| Sign-up | 282% | 13% | 309% |
| Sign-in | 417% | 3% | -22% |
| Account management | 30% | 490% | -62% |
| SMS | 7,907% | -66% | 835% |

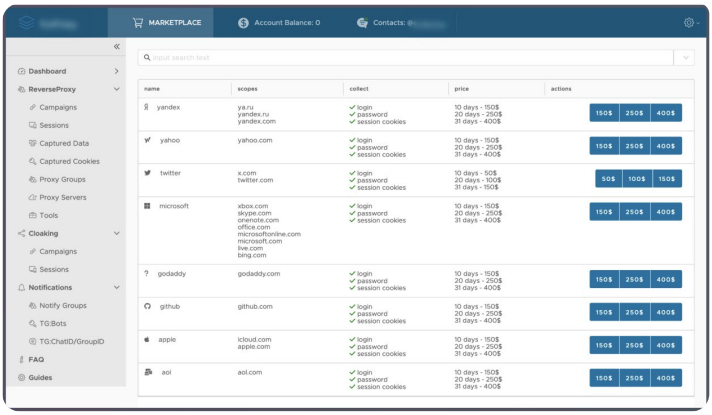
**Table 2: Size of Attacks: Quarter-over-Quarter Changes in Malicious Traffic by Attack Point** Table shows percentage changes from previous quarter. Read rows horizontally to track trends.

## INSIDE THE THRIVING UNDERGROUND ECONOMY

### Veiled Marble

Phishing continues to increase, with 3.5 billion spam emails sent daily. According to the FBI IC3 report launched in 2025, phishing and spoofing was responsible for more than $70 million in losses. And this is just “reported” fraud: it's likely that the true damage is much bigger.[8]

Unlike the clunky social engineering attempts of the past, today’s scammers have easy access to phishing-as-a-service toolkits like those from attack automation service Veiled Marble ($400 per month), enabling them to launch convincing reverse-proxy phishing attacks that compromise MFA by stealing session cookies through fake interactions with actual company websites.




**ABOVE:** This screenshot depicts the “Marketplace” for Veiled Marble. This is where scammers are able to purchase individual sites for services (as Veiled Marble calls them) to attack.

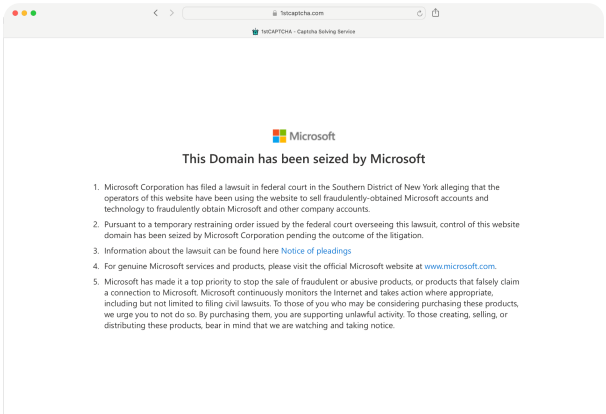
### Greasy Opal

Cyber attack enablement businesses like Greasy Opal are supercharging the careers of even inexperienced cybercriminals, offering inexpensive ways for financially motivated scammers to launch attacks. Groups like these provide AI-built bots and tools with machine learning algorithms for CAPTCHA solving at scale.


**ABOVE:** This screenshot of Greasy Opal’s primary tool that uses image recognition and ML to attempt to solve CAPTCHAs that have been deployed to protect consumers online accounts.

### Storm-1152

All companies are at risk from organized fraud networks that flood networks with spam, cause financial harm and erode consumer trust. For example, Vietnam-based Storm-1152 created 750 million fraudulent Microsoft accounts, amounting to millions in revenue, before the Microsoft Digital Crimes Unit and Arkose Labs ACTIR unit collaborated to neutralize the threat.




**ABOVE:** Screenshot showing what scammers saw when attempting to access the Storm-1152 website on the day of its disruption.

[8] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

# HOW ATTACK TYPES ARE EVOLVING

Scammers are evolving strategically, with fake account creation emerging as their dominant tactic. This vector grew from 53% of all attacks in Q1 to 61% of all attacks in Q4, reflecting its effectiveness for enabling money laundering and financing illicit activities. The malicious traffic (a measure of the size of attacks) associated with fake accounts surged throughout the year, with a 1,652% increase from Q1 to Q4 and growth (330%) in the final quarter over Q3.

Raw attack numbers tell an equally compelling story, with fake account creation initially dipping 22% in Q2 before a strong 39% increase in Q3 and continuing upward with a 14% gain in Q4. This consistent upward trajectory in number and intensity during the second half of the year suggests scammers are heavily investing in this attack type due to its consistently high returns and scalability.

SMS toll fraud, while representing a smaller portion of total attacks, showed the most dramatic growth trajectory of any attack vector. It started at just under 4% of all attacks in Q1 and grew to nearly 9% by year-end. The attack volume reinforces this alarming trend, with consistent quarter-over-quarter growth of 40% (Q2), 18% (Q3), and a particularly steep 53% jump in Q4—resulting in the number of attacks more than doubling over the year. This steady acceleration in number and intensity reveals scammers' growing confidence in this attack vector as they perfect their techniques. This meteoric rise indicates scammers' opportunistic exploitation of newly discovered vulnerabilities. One rideshare giant hemorrhaged $2.5M annually to SMS toll fraudsters until specialized detection measures stanched the bleeding.[9]

In-app threats present a fascinating contrast, showing a steady decline in volume while simultaneously increasing in attack size. This attack type dropped from 15% of all attacks in Q1 to just 7% by Q4, with raw attack numbers falling to a 52% decrease in prevalence. Yet despite fewer attacks, the malicious traffic (attack size) associated with in-app threats increased by 192% throughout the year, revealing the efficiency of scammers (fewer but bigger attacks). This precision targeting demonstrates scammers' evolving capabilities to identify and exploit high-value opportunities within applications while maximizing the impact of each attack. Online Travel Agencies (OTAs) exemplify this trend. By year's end, scammers were spending 80% of their efforts on in-app threats as stronger account creation defenses pushed attackers toward vulnerabilities in stored payment data—a classic example of scammers adapting to security improvements by seeking new paths of least resistance.

| | Quarter 1 | Quarter 2 | Quarter 3 | Quarter 4 |
|---|---|---|---|---|
| Fake Account Creation | 53% | 49% | 55% | 61% |
| ATO | 26% | 29% | 25% | 19% |
| In App Threats | 15% | 14% | 11% | 7% |
| SMS Toll Fraud | 4% | 6% | 6% | 9% |

**Table 3: Attack Type Distribution: How Scammers Shifted Their Focus Table** shows percentage distribution of attacks by the four major attack types for each quarter. Read columns vertically to track scammers' quarterly priorities.

[9] https://www.arkoselabs.com/resource/how-a-rideshare-giant-balances-sms-toll-fraud-security-with-great-user-experience-case-study/

Meanwhile, account takeovers (ATOs)—while still persistent—dropped as a percentage of overall attacks, from 26% of all attacks in Q1 to 19% of all attacks in Q4. This shift shows scammers' pragmatic approach to cybercrime; they prioritize methods with higher success rates, lower detection risk and better scalability. They respond to defensive measures not by abandoning efforts but by reallocating resources to maximize their attack ROI. The number of attacks confirm this trend, with ATOs declining nearly 5% from Q1 to Q2, briefly surging 8% in Q3, then plummeting 22% in Q4—a clear indication of scammers pivoting their tactics as the year progressed. However, the actual malicious traffic (size of attack) associated with ATOs grew by 296% from Q1 to Q4, suggesting that while ATOs may be less prevalent proportionally, they remain a significant threat with increasing sophistication.

These evolving patterns reveal scammers' pragmatic approach to cybercrime. Rather than abandoning efforts when faced with enhanced security, they skillfully reallocate resources toward more vulnerable attack vectors, constantly rebalancing their portfolios to maximize ROI. The data paints a clear picture: scammers operate as agile business entities, swiftly adapting their strategies based on shifting security landscapes and potential returns.

| | Q2 over Q1 | Q3 over Q2 | Q4 over Q3 |
|---|---|---|---|
| Fake Account Creation | 270% | 10% | 330% |
| Account Takeover (ATO) | 378% | 4% | -20% |
| In App Threats | 30% | 490% | -62% |
| SMS Toll Fraud | 13,304% | 40% | 19% |

**Table 4: Evolution of Attack Strategies: Quarter-over-Quarter Changes in Malicious Traffic.** Table shows percentage changes in size of attacks from previous quarter by attack type. Read rows horizontally to identify trends in scammer tactics.

**60%**
OF ALL ATTACKS IN Q4 WERE SMS TOLL FRAUD

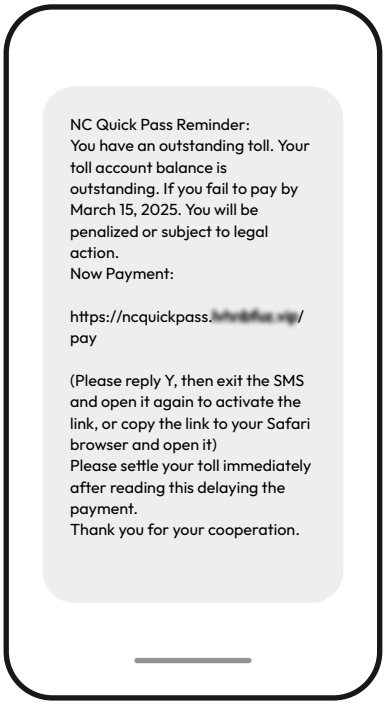
**Fintech:** SMS toll fraud targeting fintechs exhibited a dramatic transformation in 2024, exploding from 0% of all fintech attacks in Q1 to 60% of all fintech attacks by Q4. The malicious traffic (attack size) data reveals an even more striking pattern—SMS toll fraud surged from just over 5% of total fintech malicious traffic in Q1 to a dominant 51% in Q3 before settling at 23% in Q4. One likely explanation? Enhanced KYC protocols and regulatory pressure forced attackers to pivot toward SMS verification weaknesses. As regulatory pressure intensified and account creation defenses improved, attackers adaptively exploited SMS verification weaknesses.

**75%↑**
**Q4oQ3**

**Media:** The media industry became ground zero for MFA compromise attacks with attack numbers and malicious traffic surging. The number of these attacks—also known as adversary-in-the-middle reverse proxy phishing—jumped 75% from Q3 to Q4, but even more striking was their intensification, with malicious traffic skyrocketing from tens of thousands to millions in the span of roughly 90 days. This dramatic shift suggests scammers identified a psychological vulnerability unique to media consumers, who often perceive streaming accounts as relatively low-risk and hastily approve MFA prompts to quickly access desired content.

# ATTACK MECHANISMS: CALCULATED ECONOMIC DECISIONS

The data reveals a calculated shift in scammer attack mechanisms toward more sophisticated techniques. Bot malicious traffic—the size of attacks—is growing at an alarming rate (176% in Q2 over Q1, 25% in Q3 over Q2, and 173% in Q4 over Q3), but advanced bot malicious traffic is growing even faster (339% in Q2 over Q1, 96% in Q3 over Q2, and a staggering 556% in Q4 over Q3). Tactics for using these mechanisms are constantly evolving to exploit consumer fear and confusion—as evidenced by the 800% increase in bot-generated toll text scams targeting even U.S. residents where no toll roads exist.[10] The new FBI IC3 report reveals citizens lost $129,624 in 2024.[11]




Looking at trends in the number of attacks reveals equally telling patterns. Advanced bot attacks showed consistent quarter-over-quarter growth in frequency, increasing 57% from Q1 to Q2, then surging 73% in Q3, before stabilizing with a modest nearly 3% growth in Q4. This growing pattern of sophisticated attacks indicates that scammers are increasingly investing in advanced technological capabilities that deliver higher returns on their criminal investments, allowing them to execute more complex and effective attacks against enterprise security systems.

A volatile pattern suggests human fraud farms remain viable when conditions are favorable, with bad actors rapidly scaling operations up or down based on defensive countermeasures and profit opportunities. This volatility is evident in the malicious traffic data, with human fraud farm malicious traffic surging 957% in Q2, plummeting 92% in Q3, then increasing dramatically with a 599% increase in Q4. Threat actors appear to be strategically deploying human fraud farms alongside automated alternatives, selecting the most profitable method for specific targets and timeframes. For example, the dramatic fluctuations in attack traffic mirror operations in Myanmar's scam centers, where criminal groups quickly adapt to enforcement pressure by relocating workers or temporarily suspending operations during crackdowns.attacks against enterprise security systems.[12]

Of special note are gig economy platforms, which experienced a surprising return of human fraud farm attacks in Q4 after they had disappeared entirely in Q3. The combination of high accessibility (consumer-facing apps) with valuable targets (like payment details) creates multiple profitable attack vectors that justify a diversified tactical approach.

**Attack automation services** represent another dimension of scammers' pragmatic approach. These tools—developed by experienced cybercriminals and sold to less technically skilled individuals—lower the barrier to entry for scams, creating a vibrant black-market economy. The data shows that after explosive growth in number of attacks (231% Q2 over Q1) and malicious traffic (2,046% in Q2 over Q1), these services peaked at 26% proportionally of all malicious traffic in Q2 before declining sharply to just 6% by Q4. This pronounced rise-and-fall pattern demonstrates scammers' ruthlessly experimental approach and willingness to abandon unprofitable methods. Case in point: Veiled Marble discontinued its phishing kit against a tech company with strong defenses rather than trying to circumvent them, showing how threat actors continuously test and refine based on effectiveness metrics.

[10] https://www.arkoselabs.com/latest-news/toll-text-scam-on-the-rise-what-las-vegas-drivers-need-to-know/
[11] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[12] https://www.bbc.com/news/articles/c2d3w90x86po

| All Industries by Quarters | Malicious Traffic | | |
|---|---|---|---|
| **Attack Mechanism** | **% change Q2 - Q1** | **% change Q3 - Q2** | **% change Q4 - Q3** |
| Advanced Bots | 339% | 96% | 556% |
| Attack Automation Services | 2,046% | 25% | -35% |
| Bots | 176% | 25% | 173% |
| Human Fraud Farms | 957% | -92% | 599% |

**Table 5: Shifting Tactics: Quarter-over-Quarter Changes in Malicious Traffic by Attack Mechanism.** Table shows percentage changes in attack size from the previous quarter for each mechanism type. Note the massive initial growth in attack automation services (2,046%) and the dramatic volatility in human fraud farms, reflecting scammers' agile tactical adjustments.

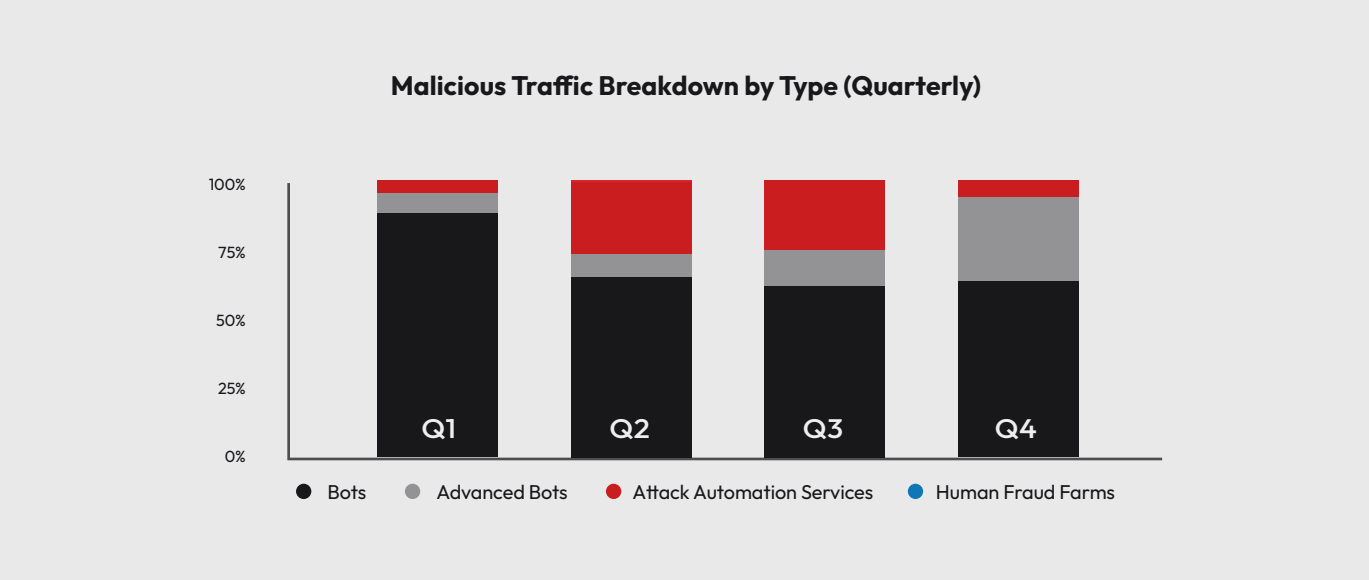



**Chart 1:** The proportional distribution of malicious traffic by attack mechanism across quarters. Note how bots consistently dominate the landscape while advanced bots gain significant share in Q4.

**46%**
OF MALICIOUS TRAFFIC WAS FROM ADVANCED BOTS

**Airlines:** This sector exhibited a fascinating evolution in understanding scammer behavior and attack patterns throughout 2024. While initially following cross-industry trends with a mixed approach in Q1, airlines faced almost exclusively bot attacks during Q2-Q3 (100% in Q2 and 99.99% in Q3). The most revealing transformation occurred in Q4, when scammers upped their game. Advanced bots suddenly represented more than 46% of all malicious traffic—a complete strategic pivot by scammers. Combined with the conspicuous absence of attack automation service malicious traffic in Q2 and minimal presence in other quarters, this suggests threat actors see unique opportunities in the airline industry that warrant customized, highly targeted strategies rather than commoditized attack toolkits.This precision approach likely targets flyers' valuable customer loyalty accounts.

**82%**
**OF MALICIOUS TRAFFIC WAS FROM BOTS**

**Gaming:** Bots remained the overwhelming attack mechanism of choice on gaming platforms throughout 2024, representing 82% of malicious traffic (attack size) in Q4. This consistency starkly contrasts with the volatile patterns seen in other industries. While advanced bot usage steadily increased from 4% of malicious traffic in Q1 to 14% of malicious traffic in Q4, bot usage by scammers maintained dominance in terms of size and number, accounting for nearly 85% of all gaming attacks in Q4. Attack automation services showed moderate growth from almost 2% of malicious traffic in Q2 and then more than 5% of malicious traffic in Q3 before stabilizing at nearly 4% in Q4. This strong preference for bot attacks likely reflects the gaming industry's lucrative combination of digital currencies, tradable assets and younger demographics less likely to recognize and report fraud—creating a perfect environment for high-volume scams at scale.

## AI-POWERED THREATS

Just as businesses are benefiting from AI, so are scammers—who have a head start. A recent Arkose Labs study on the intersection of AI and cybersecurity reveals that 88% of companies have observed an increase in scammers using AI-powered bot attacks within the last two years, and yet only 1 in 5 reported feeling very well prepared to defend against these growing threats.[13]

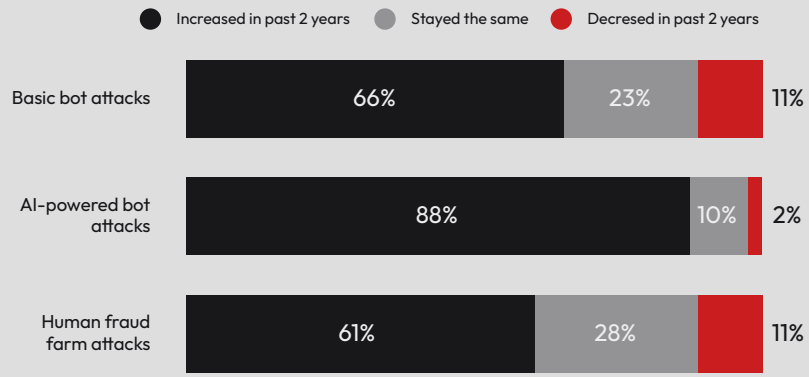



**Chart 2:** Survey question: Estimate to the best of your knowledge how attacks using basic bots, AI-powered bots and human fraud farms have changed from 2 years ago.

**How AI is being weaponized:**

- Scammers are using AI to mimic genuine consumer activity in account takeovers and to launch personalized phishing attacks.
- Malicious bots abuse LLM platforms, scraping prompts and pilfering proprietary data.
- AI empowers scammers to circumnavigate barriers in attacks, with machine learning that supercharges botnets.

This all adds up to many new strings to a scammer's bow in the age of AI. Speed, scale, adaptability and personalization combine to make today's AI-powered attacks a formidable reality. Arkose Labs research shows that CISOs understand the urgency, with AI allocation in cybersecurity budgets set to increase dramatically in the coming years.

[13] https://www.arkoselabs.com/intersection-ai-digital-fraud-cyber-defenses-all-reports

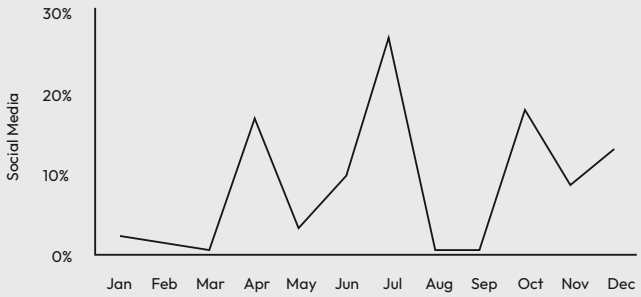
# SEASONALITY OF SCAMS

Scammers operate at an industrial scale, targeting the world's biggest brands in multiple industries. And when they see an opportunity for big financial gains, they're ready to scale. Malicious traffic, which indicates the size of attacks, climbed in the final months of the year, increasing more than 2.6X compared with Q3. And, across several industries including technology and retail/e-commerce, average attack size peaked in Q4.

**36%↑ Q4oQ3**

**Gaming:** Fall is a big season for new releases and increased purchasing ahead of the holiday gifting season. Bad actors are well attuned to trends like these, putting more firepower behind their efforts during these seasonal shifts, seeking to blend in with genuine users. Malicious traffic increased by 36% in Q4 compared with Q3.

**Social Media:** This industry saw an attack spike in October, most likely because of the U.S. presidential election. This demonstrates that bad actors focused on nation state attacks and misinformation schemes can readily increase their attack volume.




**Graph 1:** The social media industry malicious traffic spiked in correlation with the U.S. presidential elections.

**8X↑ Q4oQ3**

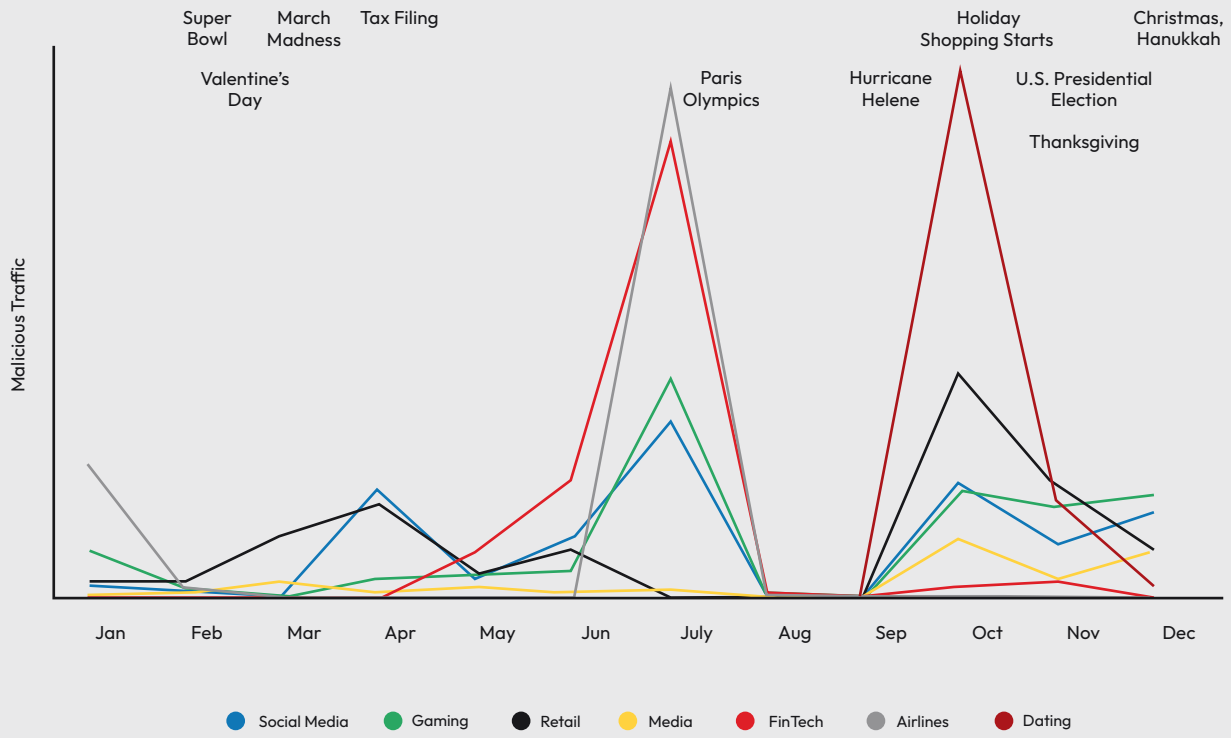
**Technology:** The data analysis reveals that the average attack sizes in this sector were dramatically overindexing compared with the relatively consistent attack sizes in other industries, with average size increasing more than 8X between Q3 and Q4. Tech is a highly lucrative industry for financially motivated scammers.

**96%↑ OF PHISHING SCAMS STOPPED**

For bad actors, frequent pivoting is the name of the game, and weaponizing automated attack services allows scammers to pump up their attack size quickly. But toolkit providers often don't retool for companies with bolstered defenses, explaining the quarter-to-quarter whiplash in attack sizes. We saw this with one major tech company, whose platform was rife with compromised traffic due to phishing scams using the PHaaS toolkit developed by Veiled Marble. After the tech company implemented the leading phishing protection solution, scams were slashed by more than 96%, and support for the popular PhaaS toolkit built for targeting the tech company came to a standstill.

# SCAMMERS HIDE IN BIG EVENTS

Scammers strategically time their attacks to blend into predictable surges in digital consumer traffic. Major events—from international games and presidential elections to natural disasters and holiday shopping seasons—create a gravitational pull for fraudsters seeking to hide their malicious activity amid increased legitimate digital activities and traffic.




**Graph 2:** These are the events around which the biggest attacks took place.

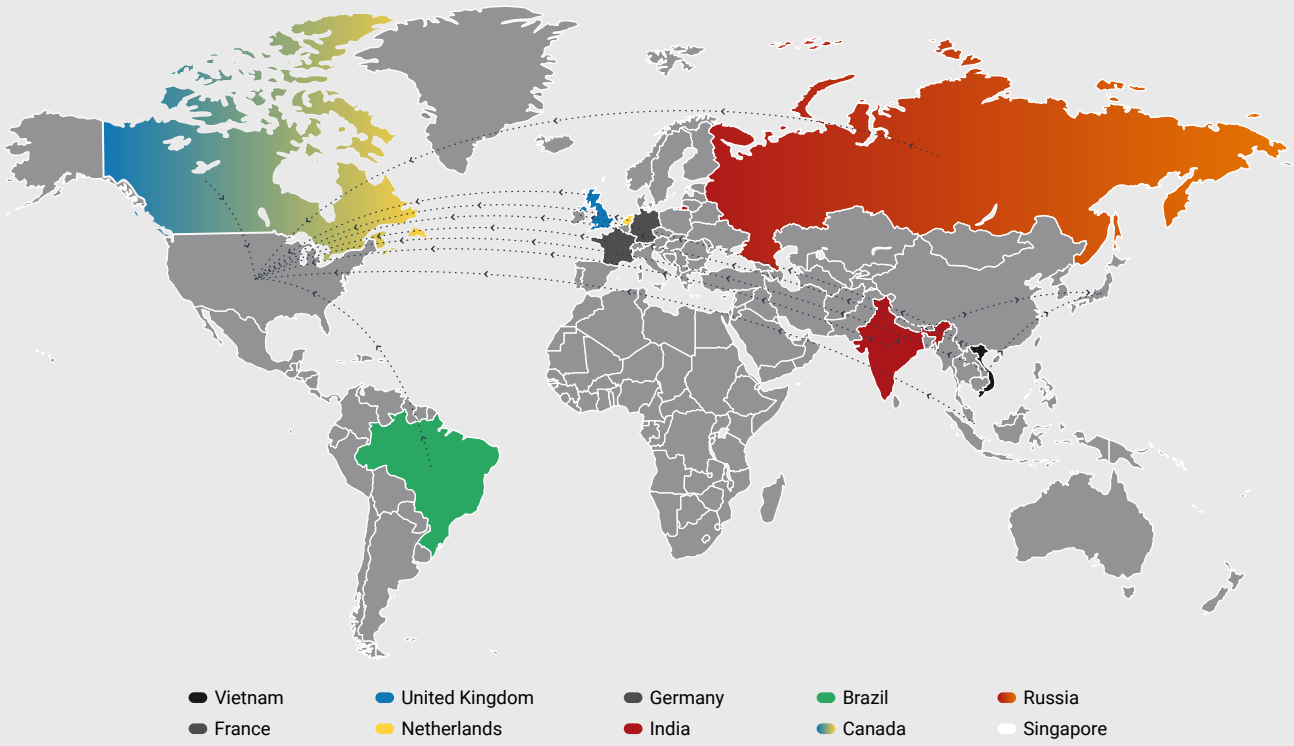
**Scammers on Holiday**. Graph 2 also reveals that scammers appeared to take a breather after the Paris Olympics and then ramped up attacks in early fall, across all industries. During August and September 2024, scammers appear to have taken an unprecedented holiday from their usual assault levels, with malicious traffic accounting for less than 1% of all annual malicious traffic.

# GLOBAL DIGITAL PROBLEM

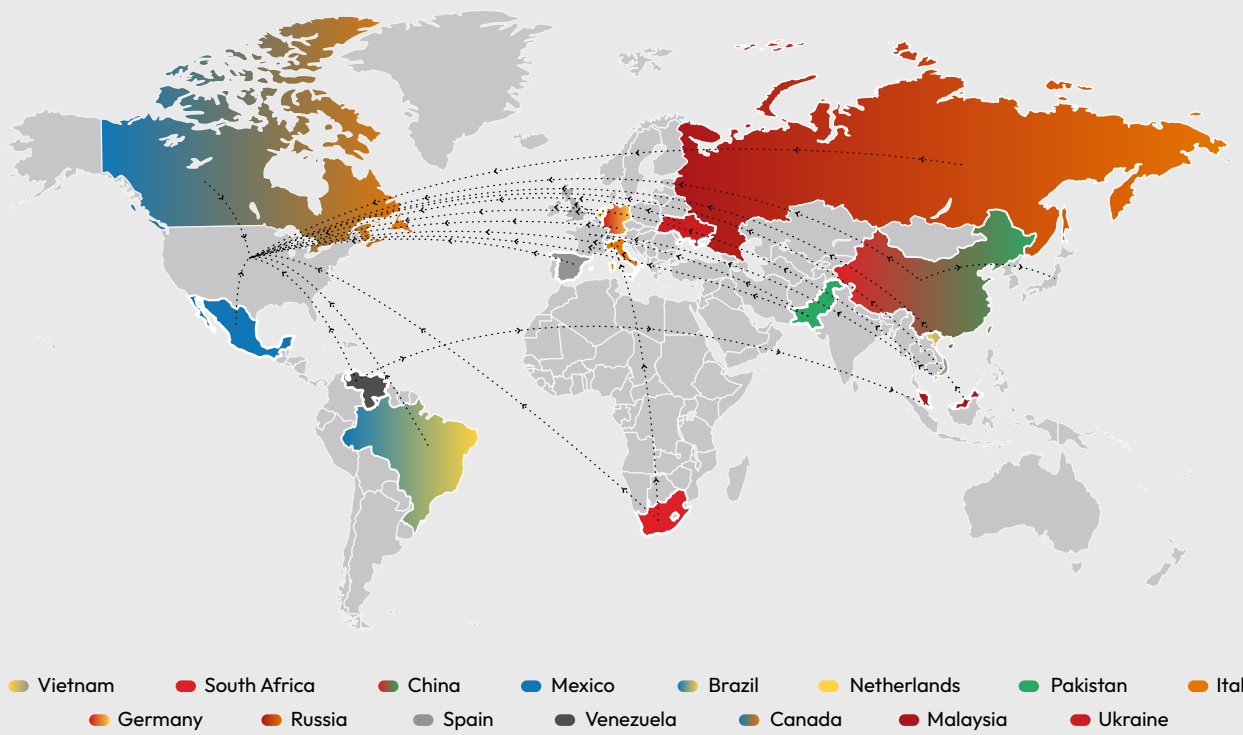
Fraud is a thriving global shadow industry. We assessed the countries where scams appear to originate, time of day and browsers used

## Countries of Apparent Origination

We took two views of the country data. The first assesses the countries where most attacks appear to originate and the second assesses where the largest attacks appear to originate.




Map 1: The top 10 countries where the most attacks appear to come from, excluding the United States.




Map 2: The top 15 countries where the largest sized attacks appear to originate, excluding the United States.

South African attackers leverage superior regional data center infrastructure to launch higher volumes of attacks than neighboring countries.

Chinese scammers target U.S. companies for massive financial gain through account takeovers, fake accounts and SMS toll fraud, exploiting valuable intellectual property with minimal risk of prosecution across jurisdictional barriers.

Much of the malicious traffic from Vietnam came from threat actor group Storm-1152, which reconstituted using AI in its attacks after being disrupted in December 2023 and attempting to set up fake accounts at Microsoft.

Pakistani scammers, motivated by U.S. sanctions and embargoes, face few consequences if caught due to limited diplomatic relations.

Russia makes the top 10 in Q4. The surge in scams and exploits originating in Russia stems from several key factors. Scammers target the wealth of financial transactions during online shopping events like Black Friday, Cyber Monday and Christmas. Enterprises inadvertently create security gaps by rushing year-end projects with reduced holiday staffing while simultaneously depleting annual security budgets or delaying updates until new allocations arrive. And finally, state-sponsored groups strategically time their campaigns to coincide with major political events and year-end policy decisions, creating a perfect storm of vulnerability. Scammers primarily lobbed SMS toll fraud attacks, set up fake accounts and took over accounts during the quarter.

El Salvador just barely missed the top 15 list of biggest attacks. The country's adoption of Bitcoin as legal currency has fueled a surge in cryptocurrency scams, as fraudsters capitalize on the nation's crypto-friendly environment to target international victims. We saw 60% of El Salvador's fraudulent traffic during Q4, and substantial shifts like this can sometimes be connected to pressures on a local level. For example, if a government is cracking down on cartel activity and crime on the streets, bad actors will pivot to online fraud, which has less harsh penalties if caught and is physically safer for the scammer.

# TIME OF DAY

To better understand some of the patterns in bad actor behavior, we examined a few interesting countries from which some of the largest attacks originated. In this analysis, we controlled for the U.S., which shows unusually large overall traffic volumes due to many attackers masking their true location to appear more legitimate when targeting American consumers and companies.

With the U.S. removed, we drilled down into the countries with the largest attacks. We looked at the full malicious traffic dataset for these heavy hitters, by quarter, day of week and time of day (in local time), assigning three categories for time of day analysis:

- **Morning/Afternoon: 8 a.m. - 4 p.m. Local Time**
- **Evening: 4 p.m. - 12 a.m. Local Time**
- **Overnight: 12 a.m. - 8 a.m. Local Time**

We sought to understand whether scammers operate as full-time professionals or moonlighters. Attack timing patterns across time zones revealed new insights into their working habits.

### Weekly Attack Distribution by Country of Origin

| Country | Mon | Tue | Wed | Thus | Fri | Sat | Sun |
|---|---|---|---|---|---|---|---|
| | Percentage | | | | | | |
| Brazil | 20% | 14% | 16% | 13% | 16% | 9% | 13% |
| China | 14% | 20% | 16% | 13% | 17% | 12% | 8% |
| Germany | 13% | 21% | 12% | 18% | 13% | 12% | 10% |
| India | 17% | 11% | 15% | 17% | 17% | 13% | 10% |
| El Salvador | 10% | 20% | 10% | 0% | 10% | 10% | 40% |
| Vietnam | 13% | 17% | 17% | 15% | 15% | 12% | 11% |
| Pakistan | 14% | 14% | 16% | 13% | 20% | 16% | 7% |
| South Africa | 16% | 14% | 13% | 15% | 17% | 11% | 13% |
| Malaysia | 13% | 17% | 12% | 26% | 15% | 9% | 7% |
| Italy | 14% | 18% | 18% | 24% | 14% | 4% | 8% |
| Spain | 18% | 14% | 15% | 16% | 21% | 9% | 6% |
| Mexico | 21% | 15% | 14% | 15% | 18% | 6% | 11% |
| Ukraine | 16% | 19% | 9% | 12% | 16% | 20% | 8% |
| Netherland | 21% | 15% | 14% | 12% | 12% | 15% | 11% |

**TABLE 6:** Data reveals distinct weekday preferences among global scammers, with most countries showing peak activity Tuesday through Friday.

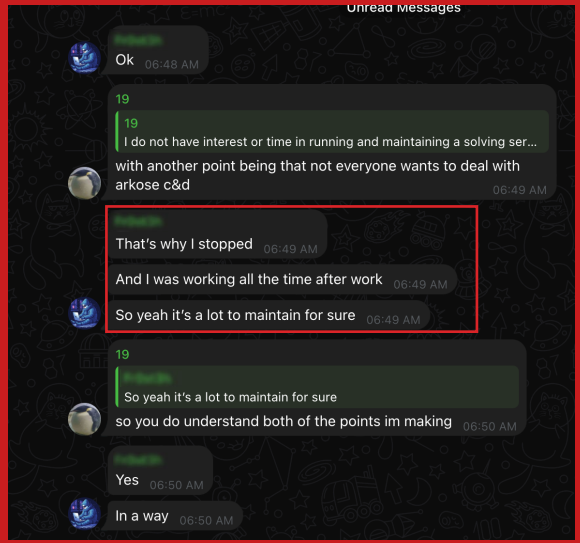
The Netherlands and Germany might not sound like major global fraud hotspots, but they were among the countries where the very largest attacks originated as measured by malicious traffic, which indicates size of attack. These countries have strong infrastructure that is attractive to scammers. Global bad actors can use reverse proxies to mount attacks utilizing the good connectivity and strong privacy of these countries. And South Africa is the only country on its continent with infrastructure suitable for launching large scale cybercrime.

## Scammer Daily Activity Patterns, by Country

| Country | Evening | Morning/Afternoon | Overnight |
|---|---|---|---|
| | Percentage | | |
| Brazil | 28% | 47% | 26% |
| China | 38% | 26% | 37% |
| Germany | 41% | 21% | 38% |
| India | 49% | 30% | 21% |
| El Salvador | 60% | 40% | 0% |
| Vietnam | 36% | 25% | 38% |
| Pakistan | 43% | 27% | 30% |
| South Africa | 46% | 36% | 18% |
| Malaysia | 35% | 30% | 34% |
| Italy | 45% | 36% | 18% |
| Spain | 47% | 29% | 23% |
| Mexico | 21% | 56% | 23% |
| Ukraine | 54% | 32% | 14% |
| Netherland | 48% | 22% | 31% |

**TABLE 7:** Analysis shows most countries conduct attacks predominantly during evening hours of 4 p.m. to midnight local time.

Spain and Italy are among the countries seeing their fraudulent traffic peak during the evening. This suggests that many scammers operating within these countries are committing fraud after a day job. Conversely, in Brazil and Mexico, larger proportions of fraudulent traffic are initiated during typical working hours. In India, where evening shifts are common, malicious traffic peaked later in the day, with 49% of attacks occurring between 4 p.m. and midnight India Standard Time.




Recent dark-web chatter supports that many scammers scam as a side hustle and that effective takedown campaigns work.

# SCAMMER SALARIES

One way attackers profit is by selling packages of confirmed account credentials, typically sold as a bundled product on the dark web and consisting of between 100 to 1,000+ accounts. Price varies based on industry. We analyzed the economics of ATOs in fintech and gaming to understand scammer remuneration. Based on our calculations of attacker income against sites with legacy protections, here is what attackers targeting five sites could expect to earn:

### Potential Earnings for Cybercriminals Targeting Different Industries

| Scammer with medium reputation, targeting fintech | Scammer with strong reputation, targeting fintech | Scammer with medium reputation, targeting bulk gaming | Scammer with strong reputation, targeting bulk gaming | Scammer with medium reputation, targeting premium gaming | Scammer with strong reputation, targeting premium gaming |
|---|---|---|---|---|---|
| **$79,376** | **$119,376** | **$169,376** | **$254,376** | **$96,576** | **$145,176** |

**TABLE 8:** The estimated annual income for attackers with varying reputation levels targeting fintech and gaming with legacy security protections.

When compared with the average annual salary for a software developer in the 15 interesting countries analyzed above (calculated using the midpoint of the typical salary range), it's not hard to see that fraud pays.

### Cybercrime vs. Legitimate Work: Financial Incentives Across 15 Countries

| Country | Average software developer salary | Does fraud pay better? | | | | | |
|---|---|---|---|---|---|---|---|
| | | Med Rep - Fintech | Good Rep - Fintech | Med Rep - Gaming Bulk | Good Rep - Gaming Bulk | Good Rep - Gaming Premium | Good Rep - Gaming Premium |
| South Africa | $30,500 | Yes | Yes | Yes | Yes | Yes | Yes |
| Netherlands | $82,380 | No | Yes | Yes | Yes | Yes | Yes |
| Mexico | $33,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| Italy | $58,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| China | $73,900 | Yes | Yes | Yes | Yes | Yes | Yes |
| Vietnam | $16,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| Pakistan | $6,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| Spain | $45,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| Malaysia | $24,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| India | $15,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| Ukraine | $36,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| El Salvador | $11,500 | Yes | Yes | Yes | Yes | Yes | Yes |
| Brazil | $31,000 | Yes | Yes | Yes | Yes | Yes | Yes |
| Germany | $72,500 | Yes | Yes | Yes | Yes | Yes | Yes |
| Morocco | $28,900 | Yes | Yes | Yes | Yes | Yes | Yes |

**TABLE 9:** Cybercriminal activities consistently outpay legitimate software development careers in nearly all analyzed countries. Only in the Netherlands does a medium-reputation fintech scammer earn less than the average developer salary.

- In Pakistan, a scammer targeting bulk gaming could earn 25x more than a software developer.
- Scammers with strong reputations in El Salvador might make 20x more attacking that same sector, versus working a software developer job.
- For scammers attacking premium gaming in Vietnam, they can earn 6x+ more than at an average developer day job.

And for scammers located in these countries, the risk of attacking the U.S. might seem small. Cybercrime is hard to catch, and harder to prosecute, leaving the risk/reward calculation a simple one for financially motivated bad actors

## SCAMMERS STRATEGICALLY LEVERAGE BROWSERS

Scammers overwhelmingly favor Chrome, using it at nearly 3X the rate of the next most common browser, Microsoft Edge. These widely adopted browsers let fraudsters maximize their reach while minimizing customization efforts. Despite mobile's growing role in daily transactions, desktop remains the preferred platform for scammers, with account takeover attacks occurring almost twice as frequently on desktop compared to mobile. This preference stems from fundamental architectural differences: web applications remain vulnerable to reverse engineering and request spoofing, while mobile apps implementing certificate pinning effectively prevent man-in-the-middle attacks.

Mobile browsers still account for about 43% of all attacks in 2024. Certain browsers like Yandex and Opera show disproportionately high attack volumes (number of attacks) relative to their market share, suggesting features scammers find advantageous or security gaps being exploited. A quick overlay of industry data shows that romance scams buck the desktop trend due to the prevalence of app-based dating—scammers use mobile the most.

## TOP 10 BROWSERS BY THE NUMBER OF ATTACKS

## TOP 10 BROWSERS BY NUMBER OF ATTACKS ON DESKTOP AND MOBILE DEVICES

| No. | Desktop Browsers |
|---|---|
| 01 | Chrome |
| 02 | Microsoft Edge |
| 03 | Firefox |
| 04 | Opera |
| 05 | Yandex Browser |
| 06 | Safari |
| 07 | Chrome Mobile |
| 08 | Headless Chrome |
| 09 | Mobile Safari |
| 10 | Avast Secure Browser |

| No. | Mobile Browsers |
|---|---|
| 01 | Mobile Safari |
| 02 | Chrome Mobile |
| 03 | Chrome |
| 04 | Microsoft Edge |
| 05 | Twitter |
| 06 | Safari |
| 07 | Yandex Browser |
| 08 | Roblox |
| 09 | Opera |
| 10 | Samsung Browser |

It's equally interesting to understand the browsers that scammers use on either mobile or desktop devices. Assessing the top 10 browsers by number of attacks and either desktop or mobile reveals a clear pattern: Chrome is No. 1 for desktops, comprising 87% of attack volume (number of attacks) while Mobile Safari is the preferred browser for scams using mobile devices, comprising 79% of attack volume.

Assessing scammer behavior and browser use by the size of attacks, a noticeable change occurred quarter-over-quarter. The largest amount of malicious traffic increased 50% in Q3 over Q2 for desktop traffic. And for mobile traffic, Q4 saw a huge spike (89% over Q3) in the size of malicious traffic through mobile devices.

# CONCLUSION

Scammers hack in at the top of the consumer digital journey (account sign-up and sign-in) and then leverage attack vectors like fake accounts, SMS toll fraud, MFA compromise and account takeovers—representing just the beginning of a far more dangerous criminal pipeline. The rapidly evolving threat landscape—evidenced by surging SMS toll fraud and advanced bot traffic—requires disrupting scammer operations at these critical points to strangle the entire fraud chain's profitability and prevent devastating downstream impacts.

When enterprises fail to stop these attacks at the top of the kill chain, the second- and third-order effects create significant legal, financial and reputational damage. Consider these sobering examples: An Australian criminal syndicate stole over $3.3 million from superannuation and shared trading accounts and then laundered $2.5 million through luxury goods purchased in Hong Kong.[14] In a more extreme case, cryptocurrency exchange Binance paid a record $4.3 billion penalty for Banking Secrecy Act violations because its ineffective anti-money laundering program facilitated transactions from ransomware hackers, countries like North Korea and Iran, and terror groups.[15]

These cases highlight a critical reality: Digital fraud is not isolated—it's interconnected with broader criminal enterprises. By implementing targeted defenses at the most vulnerable attack points and addressing the economic motivations driving scammer behavior, companies can disrupt this criminal ecosystem before it makes an impact.

Here are key defense strategies, recommendations and forward-looking guidance for protecting against digital fraud.

Effective mitigations strategies begin with several predicates.

First, in a hyperconnected dark web and dark channel world where adversaries happily share data, a data-sharing hierarchy is essential to counteract the exploit data available online. A data hierarchy should have federated threat intelligence and applicable mitigations at the pinnacle. Tier two needs to be an integrated internal data fusion exercise where internal data and salient vendor data is shared with all affected internal enterprise teams. Tier three is focused on sharing key good customer data and known threat data amongst enterprises.

### With those predicates, here are some general recommendations:

1. One, determine the workflows that either provide the most amount of potential value or are least protected and harden those first. Begin with the human element (remember the adversaries are exceptional students of human behavior) and focus on critical points of dependency on one or a limited number of individuals.

2. Two, share data within the organization: fraud teams, cybersecurity teams, marketing and customer acquisition teams, and finance teams. Much like we all create RCAs for support incidents, create and share threat information and outcomes amongst the teams so that they are aware of the latest threat vectors. These teams should baseline expected activities (AI is a great enablement tool) so anomalies are quickly detected. For example, the correlation between SMS spend (typically owned by finance) and user sign-up (typically owned by marketing) is a great baseline to identify SMS toll fraud.

[14] https://www.austrac.gov.au/case-study-money-laundering-through-cybercrime
[15] https://www.enzuzo.com/blog/biggest-compliance-fines

3

Three, train, train, train. Test your threat posture, awareness and defenses often. The best way to mitigate the human element is through knowledge and training.

4

Four, partner with supply chain partners that are in the fight and take their defenses and preparedness as seriously as you do. Ensure they are using the latest technology (AI) and have the ability to federate threat data and mitigations so that you benefit from the learnings about attacks across industries.

**Effective Defense Strategies**

- Focus defenses on the most targeted attack points: sign-up and sign-in.
- Implement enhanced monitoring for SMS verification systems.
- Deploy specialized security measures for when attack sizes peak.

**Recommended Security Measures**

- Implement layered security approaches that can respond to shifts in attack methods.
- Implement continuous monitoring solutions to detect and mitigate new attack methodologies in real time.
- Enhance security for stored payment data.

**Forward-Looking Guidance**

- Prepare for the continued rise of AI-powered attack sophistication.
- Develop defenses against LLM-enhanced social engineering attacks at scale.
- Develop strategies to counteract the economic incentives driving scammer behavior.

### Bank Slashes ATOs and Unknown Sessions

**The Problem**

One of the largest U.S. banks faced increasing unknown session rates and a multitude of bot attacks compromising consumer accounts. It placed Arkose Bot Manager between Akamai and ThreatMetrix to detect and mitigate bad traffic and anomalies.

**Attack Impact**

- Hundreds of thousands of dollars wasted on downstream detection
- Deteriorating trust between customers and the bank

**The Results**

- Major cost savings through immediate reduction in unknown session traffic
- ATOs virtually eliminated, elevating consumer confidence

### Adobe Reduces Fake Accounts While Enhancing User Experience

**The Problem**

Attackers were setting up fake email accounts for phishing and spam, and unnecessary CAPTCHAs were frustrating real users and hurting sign-up rates. Adobe implemented Arkose Bot Manager with its SOC that provides 24/7/365 monitoring.

**Attack Impact**

- Increased risk of spam and phishing from trusted Adobe domain
- Poor user experience with high challenge rates

**The Results**

- Challenge rate reduced by 80%, from 10% to 2%
- Increased detection of fraudulent accounts by 90%

### Global Payments Company Stomps Out SMS Toll Fraud

**The Problem**

SMS toll fraud was costing a rising global payments company hundreds of thousands monthly. After the company selected Arkose Bot Manager to detect, isolate and neutralize threats, SMS toll fraud attacks plummeted.

**Attack Impact**

- Millions of dollars in annual SMS fraud losses
- Legitimate customer experience harmed

**The Results**

- $3.7M projected annual savings in SMS charges
- 70.2% reduction in overall SMS volume within just 3 days

## ARKOSE LABS IS IN THE FIGHT

Every day our global team enables legitimate consumers to have a seamless experience as they work, play and live on the internet. And we're detecting and preventing the most sophisticated criminals trying to stop people and companies from the "quiet enjoyment" of the internet.

Scan the QR codes below for specific information on how we stop scammers from penetrating consumer account flows to payment all the way out to the edge.

## Arkose Labs

Arkose Labs is a leading global account security provider offering a comprehensive platform that combines proprietary device identification, phishing protection, email intelligence, scraping prevention, API security and bot management. The world's leading consumer brands—including two of the top three banks, Microsoft, Expedia and Roblox—rely on the company's unified platform to reduce customer friction while preventing account takeovers, fake account sign-ups and SMS toll fraud. 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 sabotage attacker profitability and disrupt threat actor groups like Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.

Follow the company on LinkedIn for breaking news, fresh insights and curated news.

## 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.

## The 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 2024. 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. And we calculated estimated scammer salaries, comparing with the midpoint of typical salary ranges for software developers in apparent countries of attack origin, to contextualize the financial payoff of fraud in each country.

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.]

**Contact Us**

USA

400 Concar Dr, Fl 4
San Mateo CA. 94403

Australia

T.C. Beirne Building, 315
Brunswick Street (level 4),
Fortitude Valley, Brisbane
QLD 4006

United Kingdom

167-169 Great Portland
Street, 5th Floor, London,
W1W 5PF

Costa Rica

Calle 118B San Rafael
San José, SJ 1020

India

Redbrick Offices, Tower B 2nd Floor,
Panchshil Business Park Balewadi
High Street, Off, Baner – Balewadi
Rd, Pune, Maharashtra 411045

Argentina

Avenida Corrientes 800,
Buenos Aires,
Buenos Aires C1008