Arkose Labs

Fraud & Abuse Report

Q1 2020

Foreword

As we reflect on 2019, we see some notable shifts in the threat landscape, with businesses facing new levels of complexity in fraud orchestration. Rather than looking for the quick buck, fraudsters are playing the long game, with multi-step attacks that do not initially reveal their fraudulent intent.

As the saying goes, ‘money makes the world go round’, and this could not be more true for the cybercrime underworld. Fraudsters’ unrelenting demand for fresh user credentials provides the financial incentive for cyber attackers carrying out major data breaches. When fraudsters successfully leverage the spoils from these breaches to make money, they will use the proceeds to invest in more advanced attack toolkits and greater volumes of stolen data. As a result, organizations find it increasingly difficult to defend against the barrage of attacks on their websites and apps.

The only sustainable approach to curbing the cybercrime cycle of success is adopting a zero-tolerance approach to fraud prevention. Tolerating current fraud levels as a 'cost of doing business' exacerbates the problem long-term by providing the financial incentive for fraudsters. In-depth profiling of activity across customer touchpoints helps organizations facing subtle attacks that do not show immediate tell-tale signs of fraud. When combined with targeted friction, large-scale attacks quickly become unsustainable for fraudsters who have become accustomed to circumnavigating systems that avoid putting up barriers to users.

As the latest data from the Arkose Labs platform show, attack rates are continuously on the rise. Going into 2020, the fraud-fighting community needs to finally win back the upper hand against fraudsters, protecting individuals and our society from the effects of cybercrime.

Kevin Gosschalk
CEO & Founder, Arkose Labs

Report Overview

The Q1 Arkose Labs Fraud and Abuse Report is based on actual user sessions and attack patterns that were analyzed by the Arkose Labs Fraud and Abuse Prevention Platform from Oct to Dec 2019. These sessions, spanning account registrations, logins and payments from financial services, ecommerce, travel, social media, gaming and emerging technology were analyzed in real-time to provide insights into the evolving fraud and risk landscape.

- Unsophisticated bot attacks don't result in a user session and thus have not been included in this report. The report focuses on attacks from fraud outlets that combine state-of-the-art technology with stolen identity credentials and human efforts.

- The attack patterns have been analyzed across parameters and closely investigate the mechanics of inauthentic attacks as they range from automated bots to human or 'sweatshop' driven attacks. These attacks focus on defrauding the businesses and their users through fraudulent account registrations, account takeovers or payments using stolen credentials.

- Arkose Labs uses a bilateral approach that combines global telemetry with a patent-pending enforcement challenge to profile user activity in detail and act upon data in real-time. This provides unique insights into attacker identification and classification, enabling the platform to deploy appropriate responses and countermeasures. Suspect sessions are identified when they show characteristics that have been classified as abusive or malicious by Arkose Labs, based on previous activity on other customers' digital properties.

- While Arkose Labs supports multiple use cases across the customer journey, these have been broadly grouped under account registrations, logins and payments.

Q1 Fraud Report Highlights

Record holiday shopping transactions bring record fraud levels with attacks steadily increasing throughout the quarter.

Evolving attack patterns show fraudsters using more sophisticated tools and attempting to stay under the radar by using rotation and randomization of characteristics to blend in with authentic traffic.

The key countries where human-driven attacks originated from shifted again this quarter, showing fraudsters tapping into human farms across different locations to optimize their costs.

Automated attacks are becoming more complex as fraudsters mimic good customer behavior and attempt to deploy enhanced machine vision technology to bypass challenges.

Automated attacks grew by 25% while human-driven attacks grew by 90% compared to Q2 2019

Sweatshop-driven attacks from countries like Venezuela, Vietnam, Thailand, India and Ukraine continue to grow, while these attacks from the Philippines, Russia and Ukraine have almost tripled compared to Q2

Attack volumes vary rapidly, with fraudsters attacking in short bursts across the quarter, using inconsistent timing to prevent businesses from predicting when they will be targeted.

Attacks from the Philippines and Russia almost doubled compared to Q2.

Industry Roundup

Gaming

New account fraud for gaming grew by **74%** compared to Q2.

Tourism

2X growth in holiday season traffic for travel and retail.

Social Media

82% increase in sweatshop attacks for social media.

Two out of five social media logins is an attack, with over **50%** being human-driven.

Fintech

Attack mix for financial services shifted dramatically with almost all account takeover attacks coming from automated bots.

Information Technology

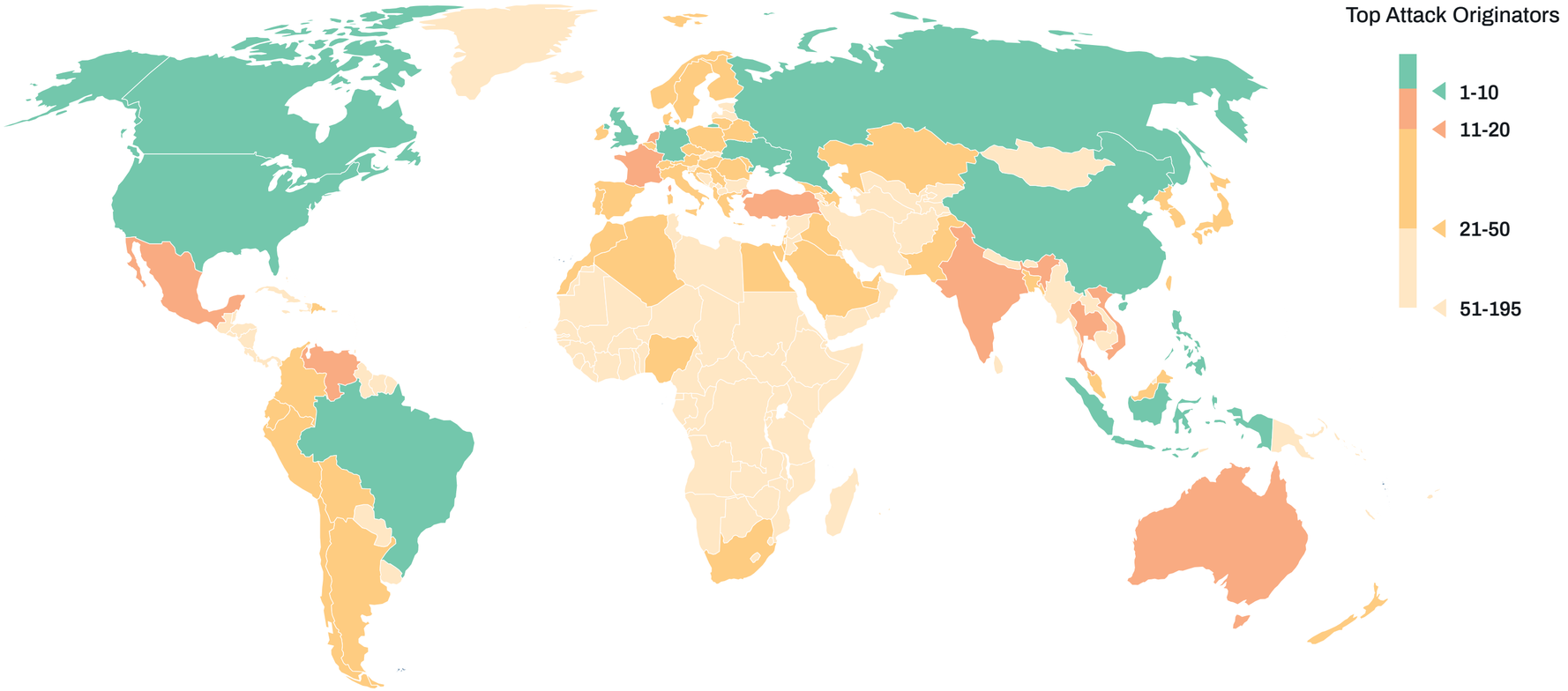
Attack rates on logins for technology platforms grew by **58%**.

Global Attack Patterns - The Race to Monetization

The globally connected nature of cybercrime is evident in the rapidly shifting attack hubs each quarter. Improvements in technology infrastructure coupled with availability of cheap labor has made certain developing economies, especially in Southeast Asia and Latin America, lucrative fraud hubs for cybercriminals everywhere.

This quarter Arkose Labs saw a sharp increase in attacks across industries and use cases, primarily from emerging economies like the Philippines, Russia and Indonesia where the attack volume nearly doubled compared to Q2 2019.

The Philippines re-emerged as the top attacker this quarter, with every third attack originating from there. These attacks target digital businesses across the globe, especially in tech, gaming and social verticals.



Top Attackers Across the Globe

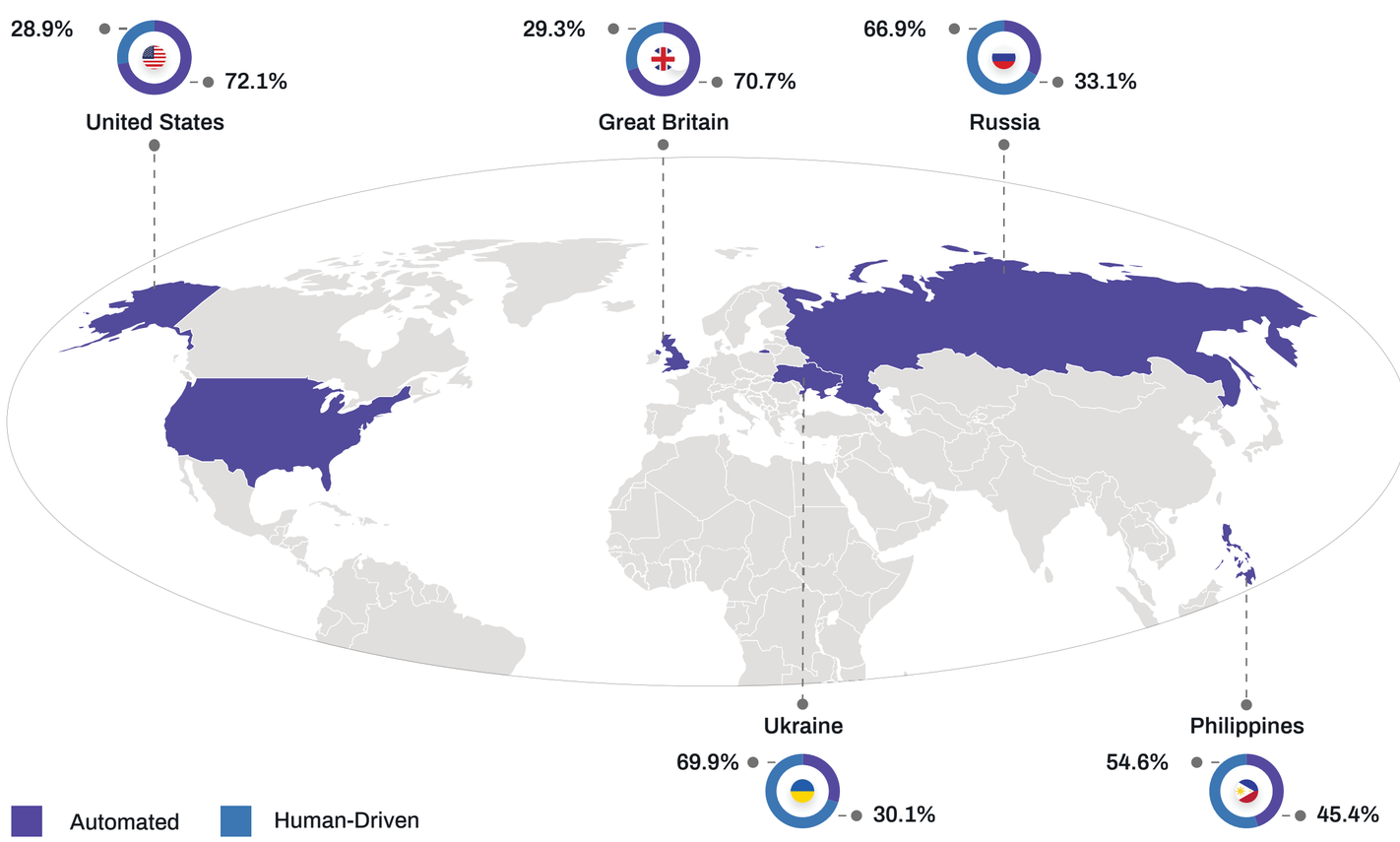
The holiday season retail extravaganza, business-driven purchasing events and a spike in year-end travel means digital commerce was at its very peak last quarter. Fraudsters around the world mobilized, looking to take advantage of busy transaction volumes in order to launch and disguise attacks.

This quarter saw a shift towards human-driven attacks. These attacks grew a whopping ~90% compared to six months prior, whereas automated attacks grew at a rate of 25%.

The growth in human-driven fraud can be attributed to fraudsters shifting their tactics in response to decreasing success rates of automated attacks, due to an increased focus on identity proofing and corroboration across industries. Additionally, many automated attacks are focused on testing or validating credentials in preparation for a more targeted human-driven attack. These testing attacks take place in the months preceding the holiday season.

This quarter, attacks from the Philippines, Russia, Indonesia, Thailand and Vietnam grew sharply, primarily from human-driven attacks.

Top Attack Originators and their Attack Mix

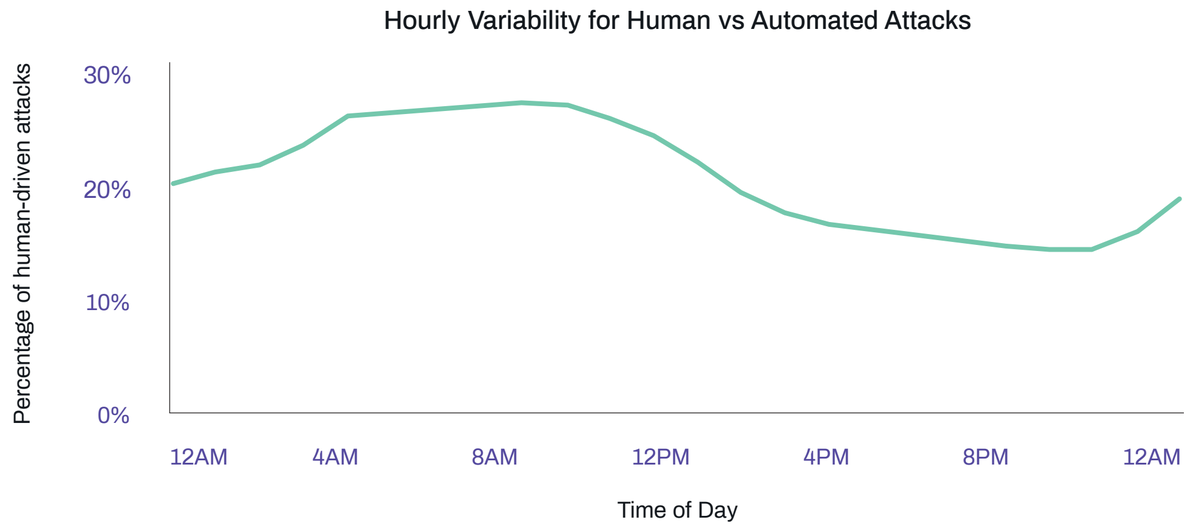


Attack Patterns Shift During Peak Commerce Season

Attack volumes were elevated this quarter, due to the availability of fresh user data off the back of recent breaches. On top of this, there was an increase in attacks targeting a select number of key business groups, demonstrating how fraudsters launch large-scale attacks on specific websites and apps.

Not only but they are also the fraudsters attacking in greater volume, they are also shifting attack patterns in order to maximize their returns during the busy digital commerce period. This quarter, peak attack timings were earlier in the day compared to the previous quarter. Consumers deviate from their normal transactional habits as they participate in the early morning rush to get the best deals during the holiday shopping season. Fraudsters will subsequently adapt their own attack timings in an attempt to blend in with spikes in legitimate traffic.

The variability of human versus automated attacks was more pronounced this quarter. Sweatshop-driven attack levels increased during the high traffic periods, with peak attack levels 50% higher than seen in Q2 2019.



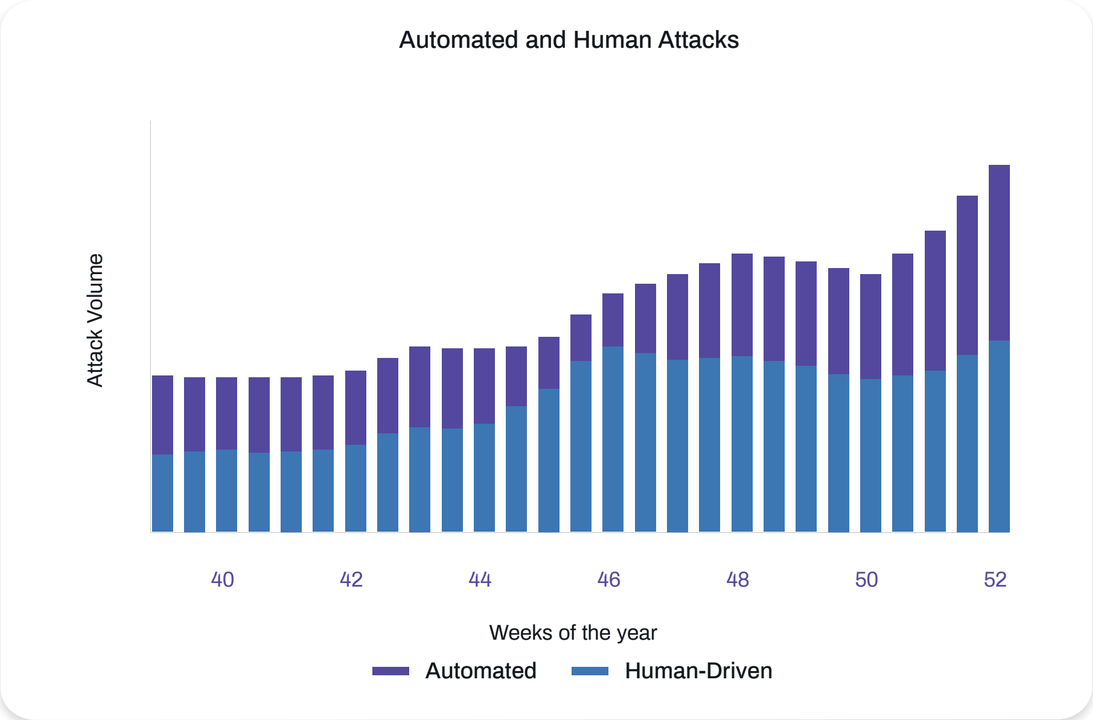
Top Four Takeaways from the Holiday Shopping Season

Heightened user engagement across all use cases, driven by promotions, deals and last-minute shopping.

Steady increase in fraudulent activity with the number of detected attacks rising notably throughout the quarter.

Shift towards human-driven attacks versus automated attacks at the end of the period as fraudsters invest in more targeted action.

Fluctuations in the attack mix show fraudsters experimenting to find the optimal blend in order to maximize return on investment.

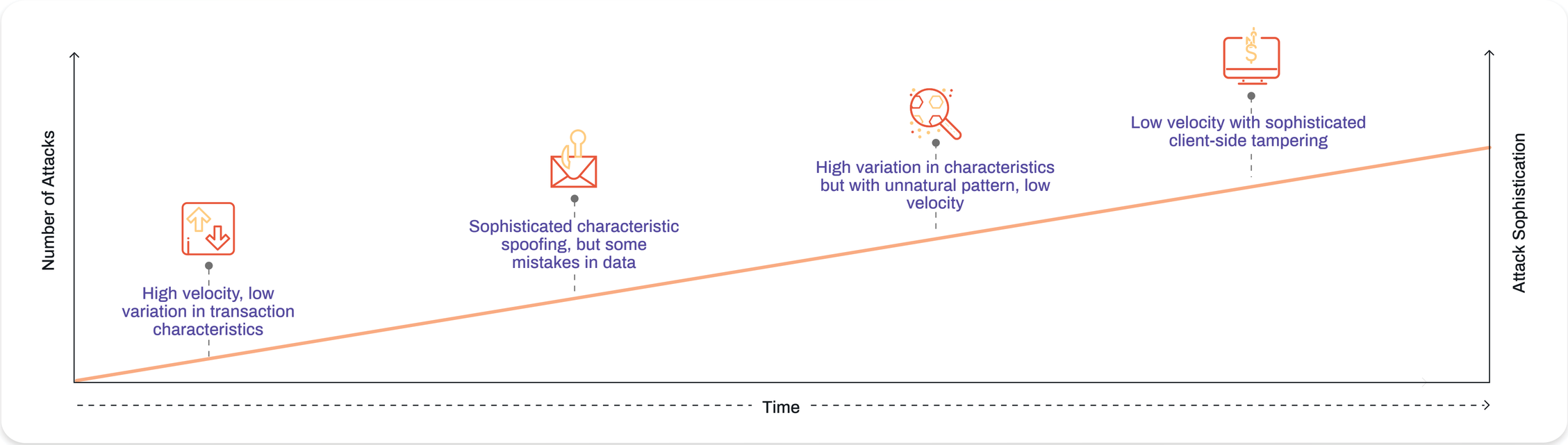


A Strategic Approach to Maximizing Fraud Returns

Digital interactions are continuing to grow at a rapid pace as more and more business models, use cases and customer interactions move online and to mobile devices. One unintended consequence of this growth has been the increase of fraud. As these transactions have grown, so had the number of attacks targeting these use cases.

What makes the situation more complex is the fact that this growth in attacks comes with increased sophistication in attack patterns. Just as businesses evolve their security stacks and defense strategies, cybercriminals are taking an increasingly strategic approach to their activity. They experiment with the optimal attack mix, from high-velocity but low-sophistication abuse to targeted attacks which accurately mimic real user behavior.

In the quest for the best return on investment, fraudsters use all the tools at their disposal, and attack patterns shift depending on whether they are deploying automated tools, human resources or a hybrid of the two. Reverse engineering of anti-fraud technologies ascertains what data systems rely on to differentiate fraud from good customers. Businesses who rely solely on data-driven fraud prevention can leave themselves vulnerable to advanced spoofing techniques and single request attacks.



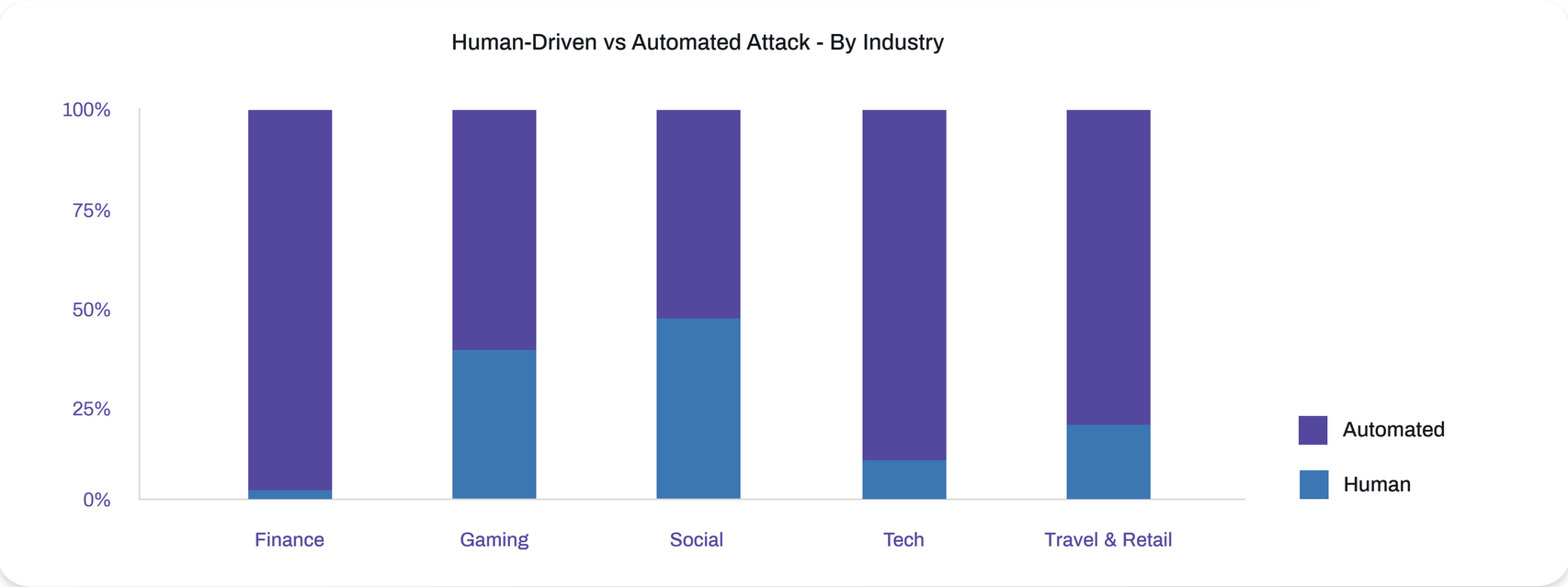
Human vs the Machine: Attack Mix by Industry

This quarter, nearly two in every five attacks were human-driven, representing a 33% increase over Q2 2019. However, the attack mix shifts greatly depending on the customer touchpoint and industry - with more human attacks when there is a higher potential of monetization.

Often automated attacks are a precursor to a sophisticated human-driven attack. The key for fraudsters is to find the right mix of human effort and bots, and tactics will change over time as more complex, multi-step attacks progress.

This quarter, we saw a big shift in financial services, with fraudsters shifting their attack patterns to primarily automated, in order to test credentials for account takeover. On the other hand, gaming, travel, retail and social continue to see a high mix of human-driven attacks, especially for account registrations.

Understanding attacks trend is vital for effective defense. The higher cost of human-driven attacks means that fraudsters will quickly abandon attack once it proves too difficult, making targeted friction highly effective against large-scale attacks.



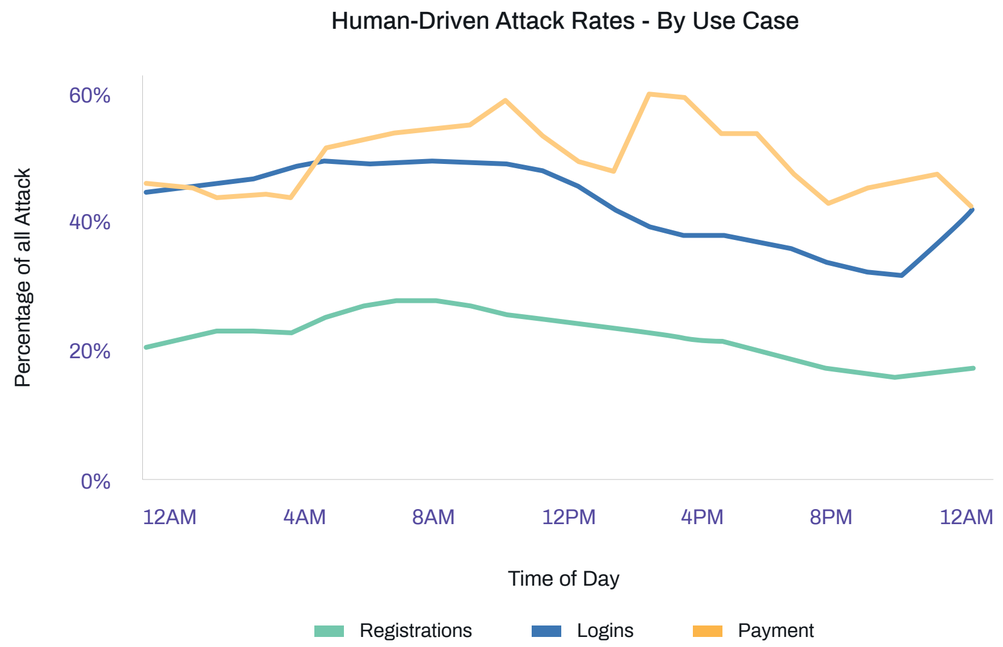
Changes to the Attack Mix Across Q4

Attacks during the period leading up to the holiday season were focused on validating and priming credentials, with a heavy reliance on automated tools to carry out new account fraud.

During Q4 the focus of attacks shifted towards account takeover and payments, with elevated rates of human-driven attacks. As digital commerce hits its busy period, many businesses adapt their risk tolerance to let as many users through as possible. Fraudsters capitalize on this move by trying to pass themselves off as legitimate customers, and leverage sweatshops to scale up human-driven attacks.

Taking over a legitimate person's account gives them instant credibility and enables them to transact freely. This quarter, human-driven attacks on account logins went up with almost half of the attacks coming from humans during peak volume times for both payments and logins.

Payment transactions continue to have the highest variability during the day, especially during peak shopping days where it's easier for fraudsters to blend in with legitimate traffic.

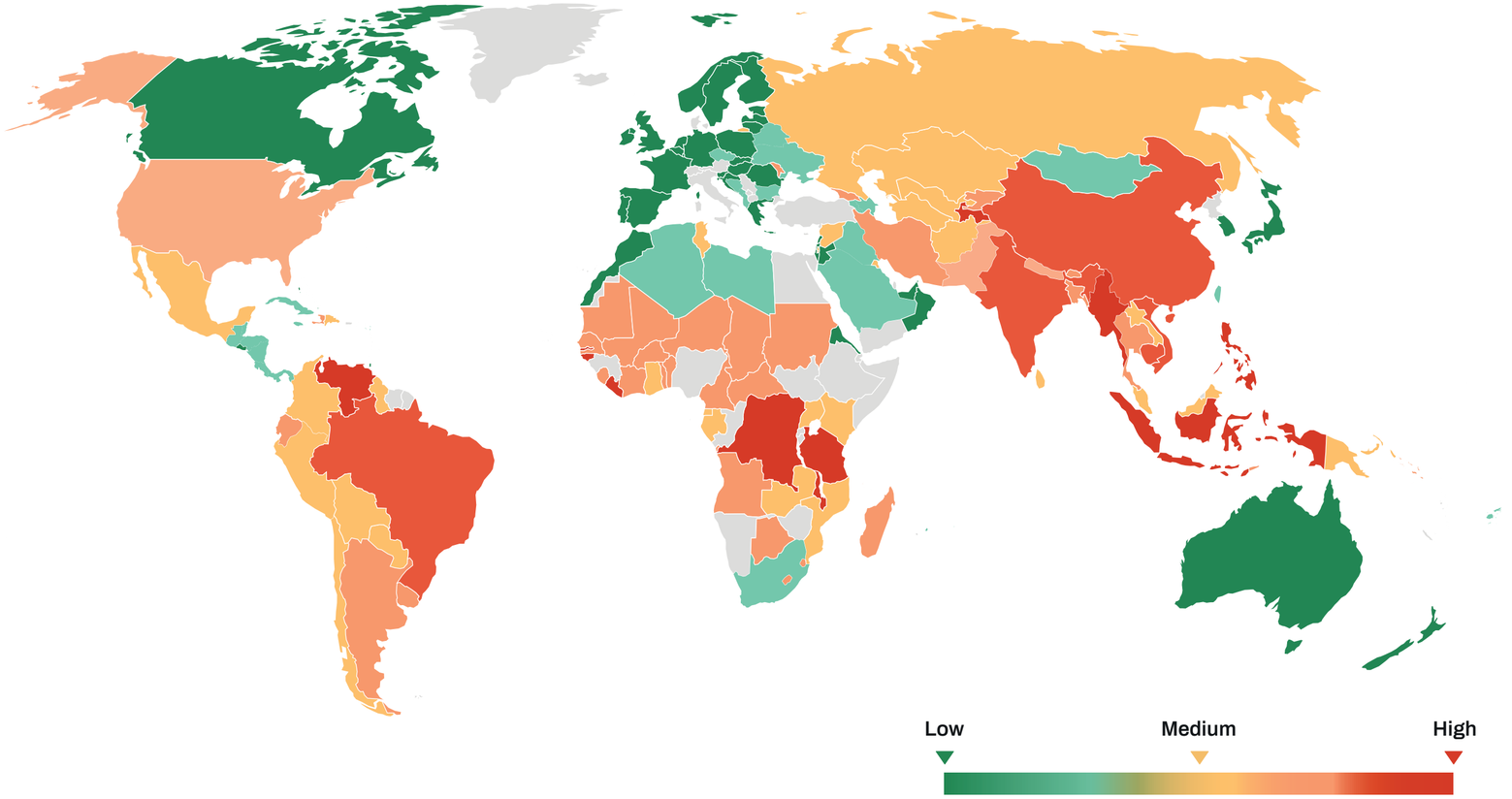


Attack Incentive Index

Disparities in wages and cost of labor, differing costs of living and the comparative purchasing power of different currencies, and access to technology shift incentive levels among would-be fraudsters.

Using regional economic indicators combined with Arkose Labs' data on known attacks, we have created an Attack Incentive Index for countries across the globe. The higher the incentive, the more resources they are likely to put behind attacks while still preserving return on investment (ROI).

Areas with high incentive levels have more financial motivation to become involved in cybercrime. They will persevere longer than average when they meet resistance or friction, before abandoning attacks.



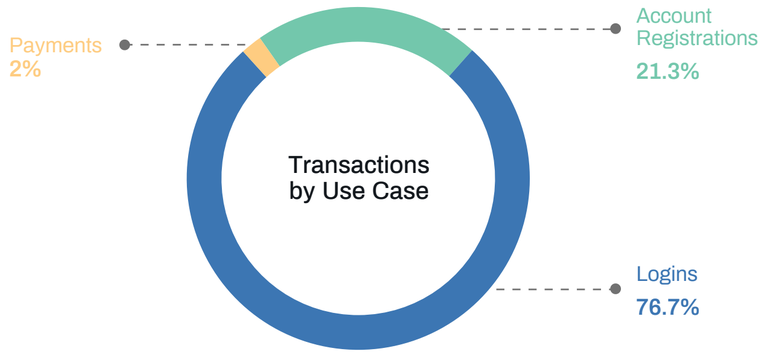
Fraud Trends Across Customer Touchpoints

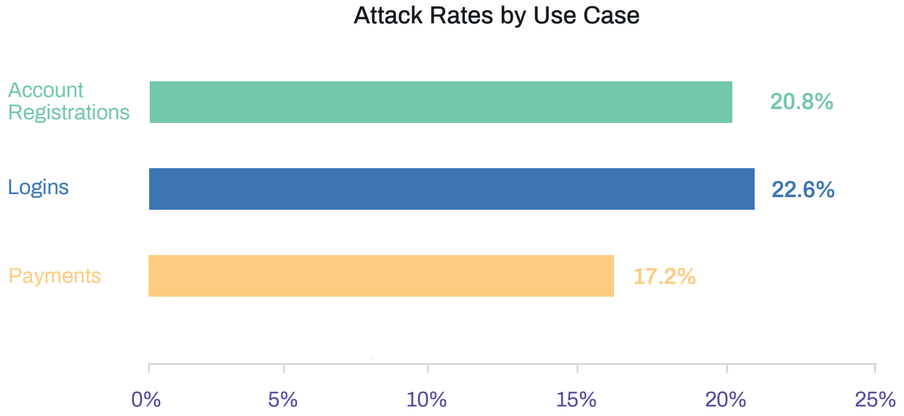
2019 was a watershed year for data breaches and its impact is seen in the growing attack rates, which grew 26% compared to Q2, primarily driven by fake account registrations, gift card fraud and account takeover attacks.

Arkose Labs works with businesses across the customer journey, with transactions being grouped under account creation, login, and payments. Nearly three out of four digital sessions are account logins. Account takeover attacks increased by 35% compared to Q2, underscoring the value of gaining access to users' accounts.

A shift in tactics was evident this quarter as human-driven account takeover attacks more than doubled compared to Q2 whereas automated account registrations increased by 90%.

These attacks may seem disconnected but are a part of a complex cybercrime ecosystem. As fraudsters find it hard to launch successful account takeover attacks using automated tools, they shift their focus to human-led attacks wherein an unsuccessful account registration attack can provide valuable insights into the existence of an account with the business, paving the way for a sophisticated account takeover attack.



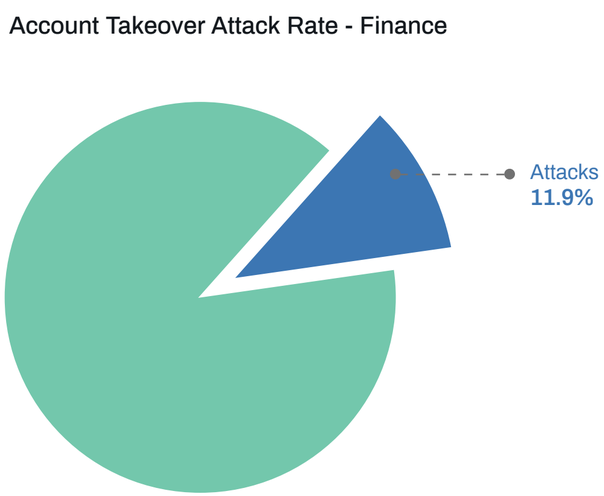


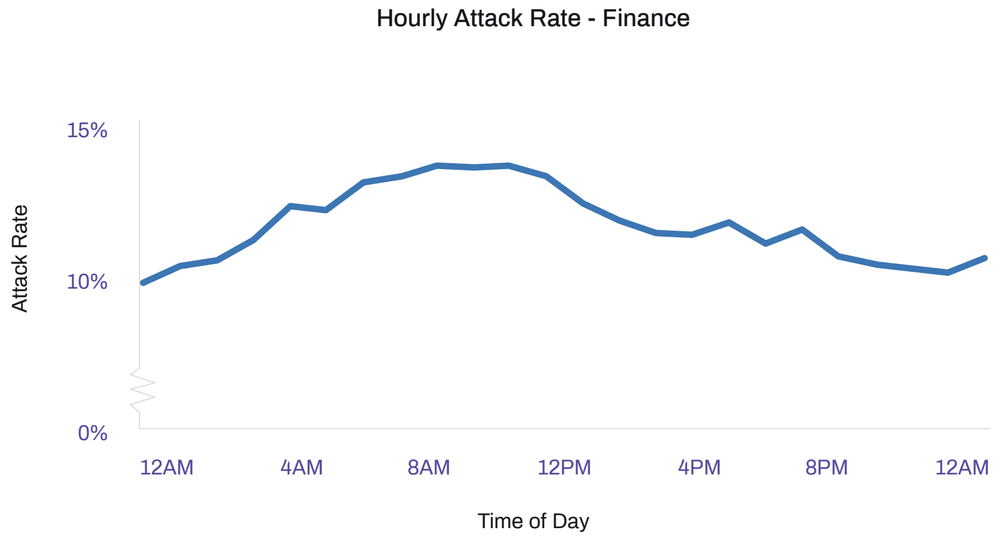
Fraud in the World of Finance and FinTech

As the financial services industry continues to transform and fintech solutions continue to gain traction, the fraud and abuse targeting digital customers is constantly shifting.

12% of financial services logins were fraud attempts. However, the overall attack levels for this sector fell this quarter compared to the previous ones, especially for human-driven attacks. This underscores the connected nature of global fraud and cybercrime. In a busy retail quarter, fraudsters will shift their resources and focus to maximize their financial returns.

Arkose Labs works with financial services providers and fintech operators to protect account logins and associated activities, including balance checks and account updates carried out on desktop and mobile applications.





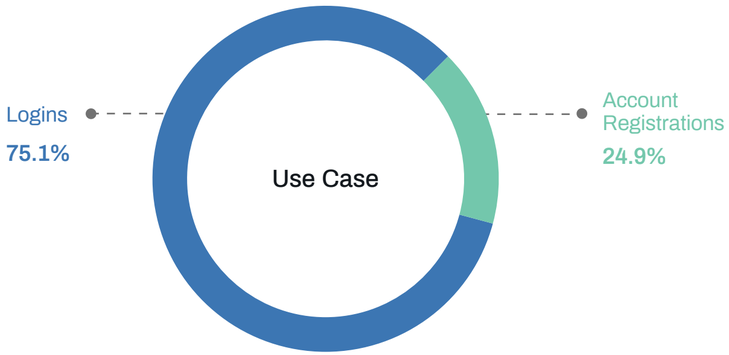
Technology Platforms Face an Array of Fraud and Abuse Tactics

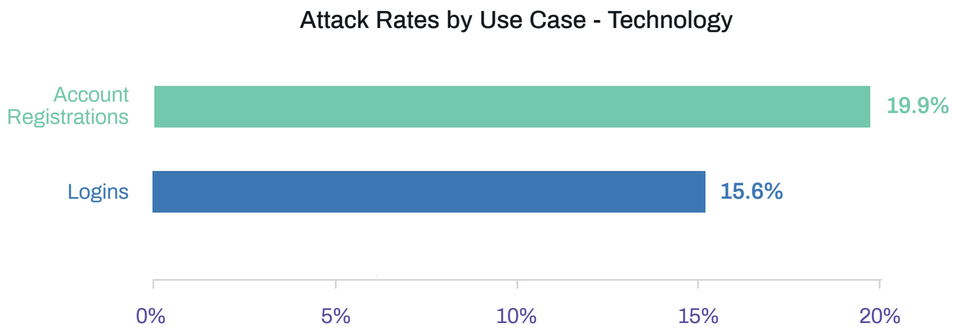
Fraud attacks on technology platforms further underscore the creative ways in which fraudsters monetize stolen credentials and resources. These platforms offer solutions to both individuals and businesses looking to leverage the convenience of communication platforms, flexible storage and office tools.

Primary use cases in this segment are account registrations and logins, with recurring payments passively funding access. These use cases are increasingly attacked by fraudsters across the globe, and this segment experiences one of the highest levels of attacks from sweatshops.

Account takeover for content scraping and spam dissemination is emerging as a big attack vector. Technology platforms also must be vigilant and protect against bad actors misusing the account registration for promotion abuse, credential testing and account resale.

More than half of new account registration fraud is human-driven, while login and scraping attacks are primarily automated. New account registration attacks on technology platforms grew 20% compared to Q2 2019, while login and scraping attacks grew 50%.

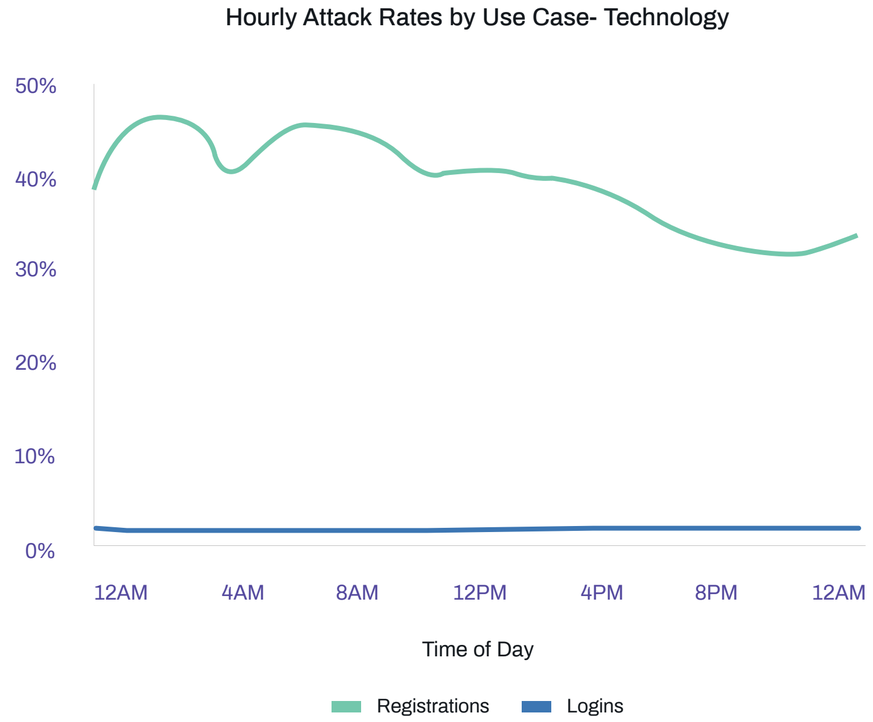


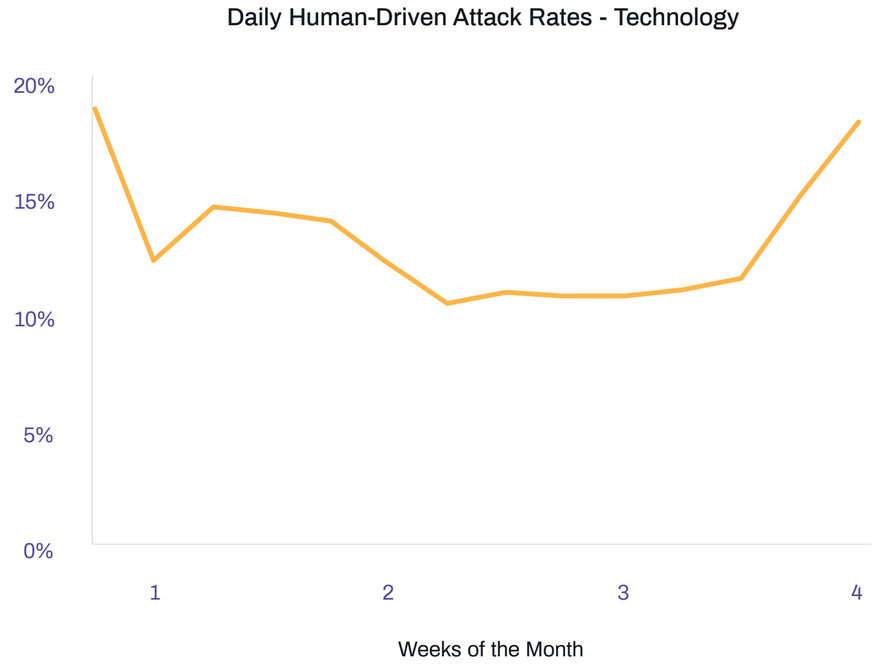


Attack Mix for Technology Platforms

Attack rates for the technology segment grew 40% this quarter compared to Q2. The human-driven attack mix declined closer to the holiday season but went up again towards the end of the year. This speaks to how fraudsters optimize their resources to focus on the best monetization potential.

Despite the overall decline, ~40% of all registration attacks are human-driven, whereas almost all of login attacks are automated.



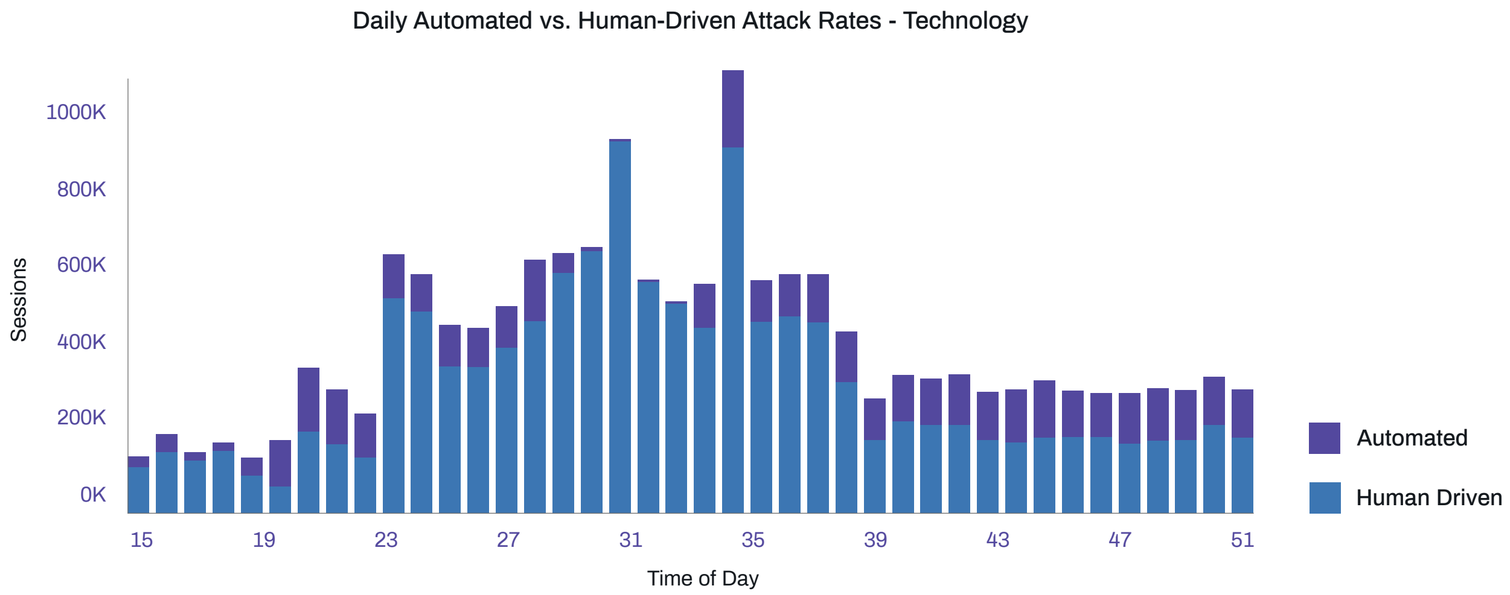


Monetizing Tech Platforms - Continued Onslaught of Human Sweatshops

Abuse on technology platform registration continues from across the globe. These attacks demonstrate the knowledge-sharing between sophisticated fraudsters that sometimes rely on sweatshops to carry out preparation activity for a larger cybercrime attack.

In the past few quarters the network has identified a series of human-driven attacks wherein fraudsters in China, U.S, India, Brazil and Russia set up fraudulent accounts to abuse promotions offering free servicer time to mine for Bitcoin. Over the quarter, the fraudsters shifted their attack patterns and locations with different regions carrying out the attacks over time.

The amount of effort a fraudster will expend is proportional to the value they get. The high monetization potential associated with bitcoin mining justifies the elevated levels of human-driven attacks, albeit from low-cost countries.

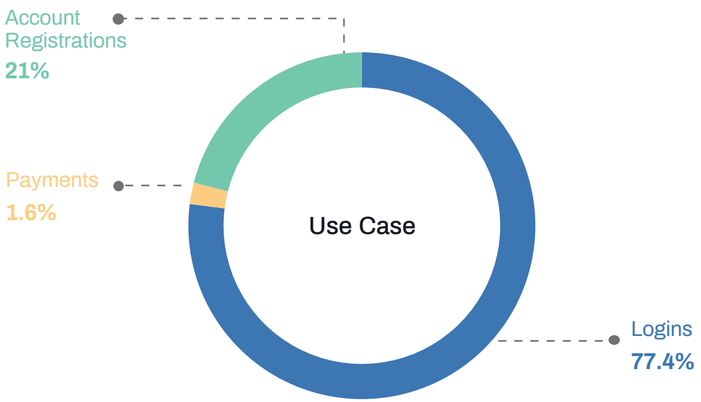


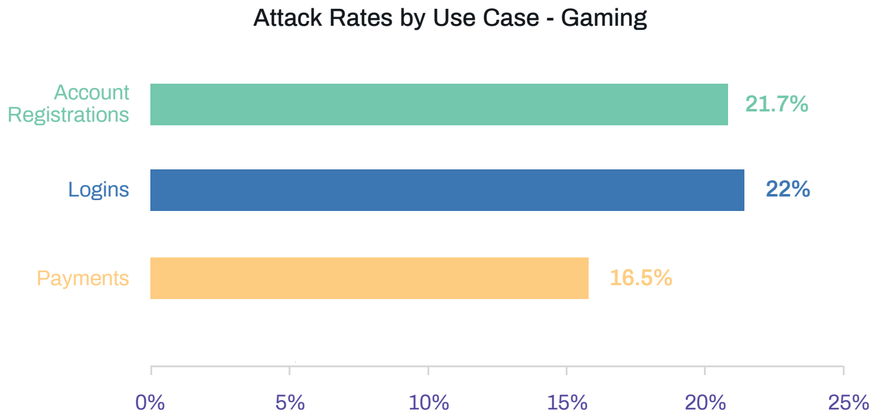
Gaming Transaction Analysis

As millions of users of all ages increasingly engage in online games, the industry has expanded and has given birth to a commerce ecosystem that has become another monetization avenue for fraudsters across the globe.

The attacks on these gaming platforms are persistent and highly sophisticated. Fraudsters use these platforms to use stolen payment methods, stealing in-game assets, abusing the auction houses and disseminating malicious content. At the same time, another sub-industry has emerged wherein fraudsters use bots to build up account profiles and sell accounts with higher levels; or target online currencies used within select games.

The overall attacks level for gaming grew 30% last quarter with most of the growth coming from new account registration attacks, which grew by over 70%.



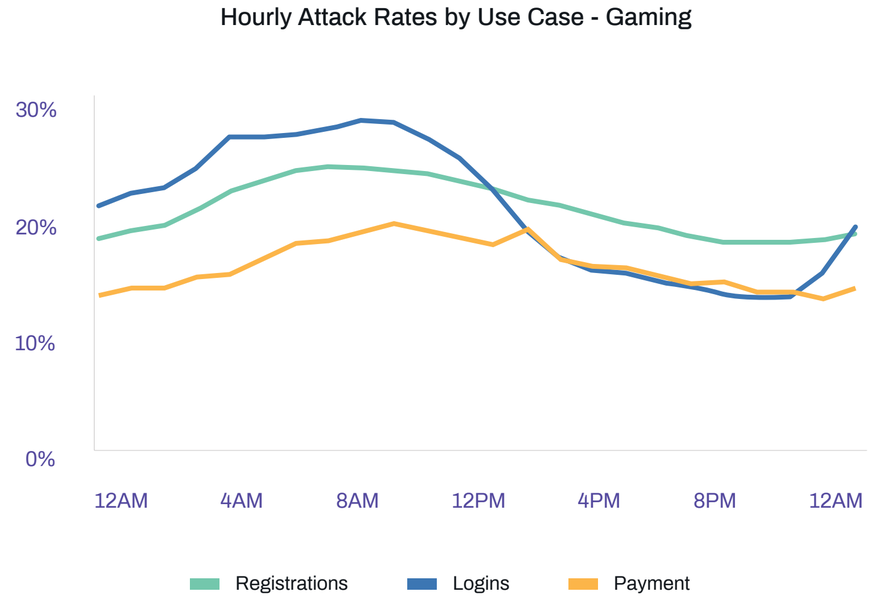


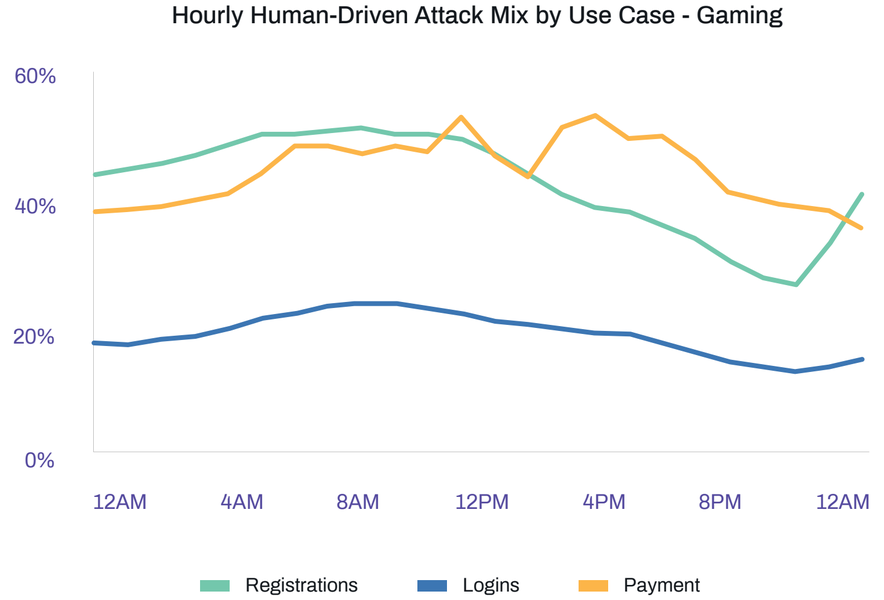
Gaming Attack Mix Variability

Attacks on gaming platforms have been primarily driven by automation, until this quarter when human-driven attacks grew sharply - especially for logins and payments. These attacks are driven by in-game spam and abuse, while payment transactions were attacked targeting in-game currency, gift-card and auction house abuse. The high mix of human-driven attacks can be attributed to the fact that these transactions require two-way interactions that automated bots can't accomplish.

Gaming attack volume varies during the day and peaks around early morning U.S. time when nearly every three out of ten logins and account registrations sessions are attacks. This peak coincides with the highest mix of human-driven account takeover attacks as well.

As with previous quarters, the attack mix stayed relatively consistent throughout the day for account registrations but had a huge hourly variability for logins and payments.





Gaming Attacks Seeing Increased Levels of Sophistication

Fraudsters are increasingly attacking gaming platforms looking for vulnerabilities with data values and events to manipulate the way they deal with any user session request.

The level of sophistication of attacks in the gaming space has evolved to client-side tampering where the fraudsters deliberately manipulate the signals being sent from their device and network, in an attempt to subvert the logic flows of businesses' fraud prevention systems.

In Q4 the Arkose Labs network detected two different, but connected, series of attacks where the fraudsters either tried to prevent the data being sent to the Arkose Labs or deliberately omitted values to avoid specific logic flows in the Arkose Labs platform.

The fact that these attacks were seen in a close time period to one another speaks to the robustness of attackers' communication networks and their ability to share information quickly.
Another testament to the connected fraud ecosystem is the sudden shift in attack origination, wherein the fraudsters quickly moved their traffic to a new location once transactions from a particular outfit were detected.

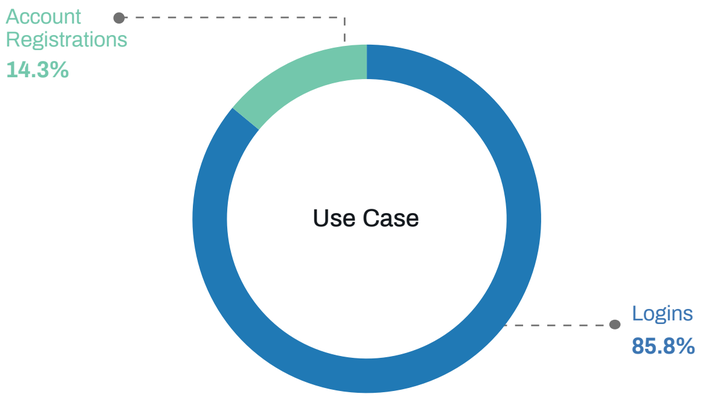
Protecting against these attacks requires a dynamic platform that can detect and mitigate these tactics, with constant innovation needed to stay ahead of the fraudsters.

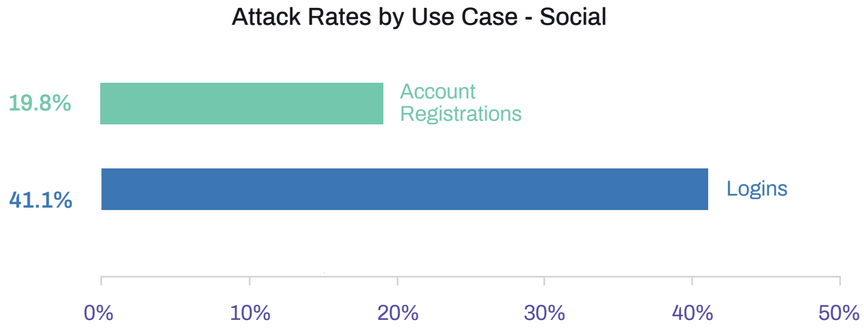
Rising Attack Volumes on Social Media Platforms

Social media platforms have reshaped the way we connect, communicate and transact online. These platforms are becoming significant commerce enablers as they permeate more and more of individuals' daily lives, across social networking, professional interactions, online dating and media consumption.

The impact of the holiday season could be seen in the higher engagement across all social media platforms. Due to the amount of rich personal data on these applications and high user activity levels, social platforms are lucrative targets for fraudsters looking to scrape content, write fake reviews, steal information or disseminate spam and malicious content.

In Q4 there was a sharp increase in attack volumes on the network for both account registrations and logins. Every two in five login attempts and every one in five new account registrations were fraudulent, making this one of the highest industry attack rates. The human versus automated attack mix also rose with more than half of login attacks being human-driven. Taking over genuine users' accounts gives fraudsters the ability to disseminate spam and malicious content as well as manipulate the accounts for indirect monetization through likes and reviews.



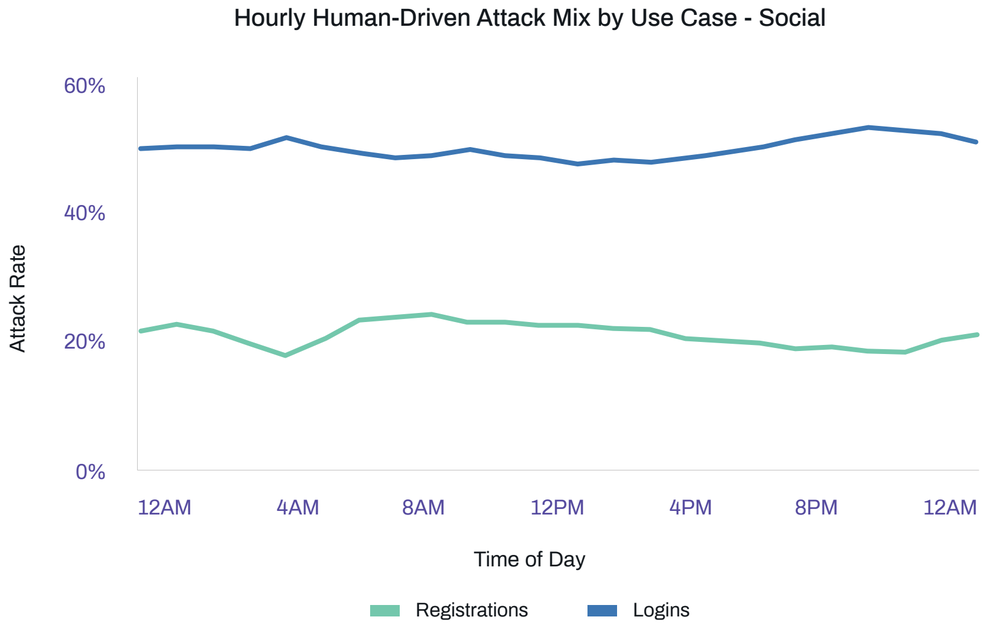


Social Media: Changing Attack Dynamics

Last quarter the attack mix for social media varied dramatically throughout the day, whereas in Q4 the mix of human-driven and automated attacks stayed very consistent.

The elevated rate of human-driven login attacks is supported by organized sweatshops, as well as lone fraudsters attempting to take over legitimate users' accounts to manipulate or steal credentials and disseminate spam.

With every two in five social media logins being an attack and over half of them being human-driven, it is clear that fraudsters target this customer touchpoint with hopes of downstream monetization.



Online Streaming Case Study: Intelligent Friction to Stop a Fraud Ring

The Arkose Labs platform detected a string of attacks on a media streaming platform, which could be connected back to a single fraud ring. Attackers varied their attack patterns, using spoofed data, stolen credentials, network manipulation and obfuscating device fingerprints and IP addresses in an attempt to avoid detection.

The fraudsters were attempting to create fraudulent new accounts, abuse promotions and disseminate spam and malicious content. The fraudsters had detailed knowledge of the parameters used to detect fraud and had the resources available to carry out multiple attacks over time while shifting their methods.

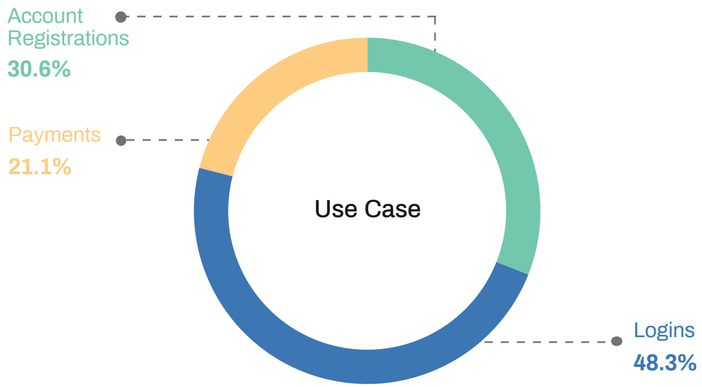
Arkose Labs was able to detect this suspicious activity by analyzing deep telltales which indicate fraud. This combined seamlessly with the challenge-response mechanism which was able to put a stop to attacks using intelligent friction. Crucially, this approach not only remediated attacks but disincentivized the fraud ring, providing long-term protection against organized attacks.

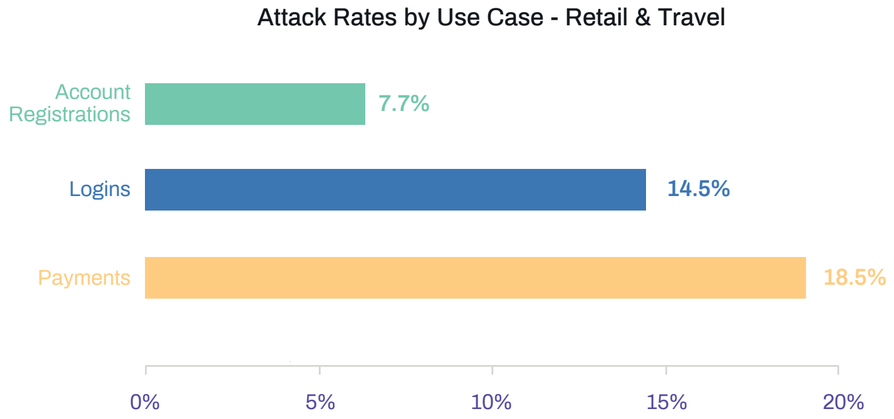
Retail and Travel - Transaction Analysis

The impact of the holiday season was evident this quarter as the overall transaction volumes almost doubled compared to the previous quarter. More customers took to their favorite e-commerce sites or travel portals to access promotions, make purchases, access their account or book travels. Q4 volumes were 3X for payment transactions, especially gift card payments.

Since most of this transaction growth was from good customers looking for holiday deals, the overall attack rates stayed flat this quarter while the total volume of attacks went up drastically.

Account takeover attacks grew 88% compared to Q3, while payment fraud went up 5X, primarily driven by automated gift card fraud. Human-driven attacks went up for both account logins and registrations but reduced by 50% for payment transactions, driven by the reduction in activity from a sweatshop targeting gift card transactions.





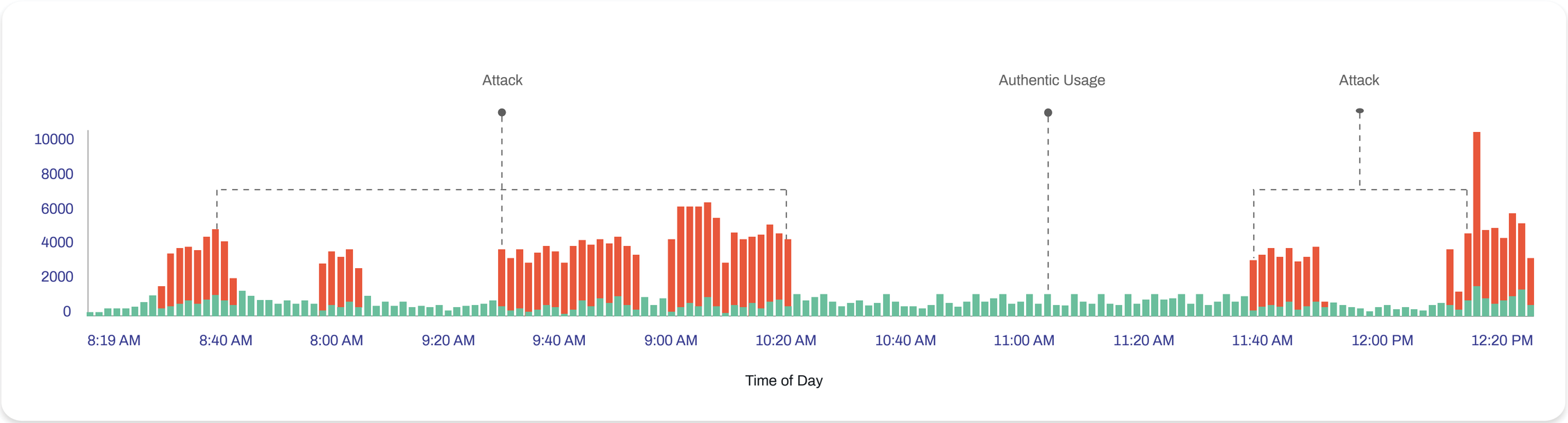
Case Study: Ongoing Sweatshop Attack on Major Gift Card Provider

An ongoing battle with a major sweatshop operation finally ceased in Q4 after a sustained fraud attack on an e-commerce provider.

The attackers were specifically targeting gift card transactions using a high volume of requests, sometimes in the levels of tens of thousands a day. These attackers were using a hybrid approach by combining automation and sweatshops to achieve both volume and sophistication at scale.

During the ongoing defense campaign, more than 30 different configuration setting measures were taken to detect attacks and continue adding friction in order to break the financial incentive of the operation.

While this had no negative impact on genuine traffic, any request from this fraud ring was given upwards of 20 iterations of a time-consuming puzzle, while also being subjected to other measures designed specifically to sap operational resources.



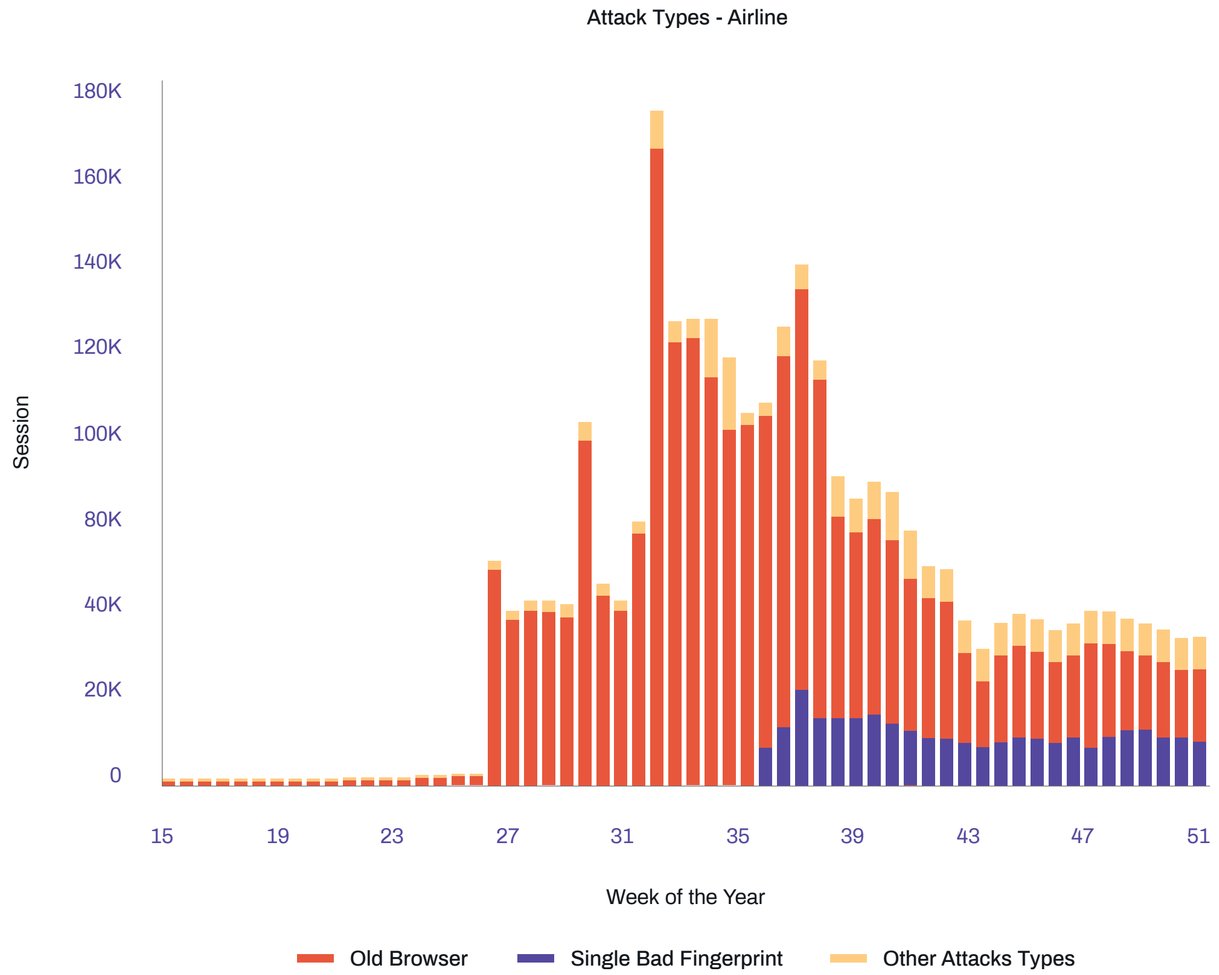
Case Study: Targeting Loyal Airline Customers

Airlines across the globe operate and manage loyalty programs to drive engagement from their high-value customers. These loyalty programs often offer air miles that can be redeemed for future travel, making them as valuable as cash in the bank.

The more loyal a customer, the higher their ‘bank balance’, making them attractive targets for fraudsters looking for a quick payday. Fraudsters looking to abuse loyalty points use a variety of tricks to fool the airline’s defenses and appear legitimate.

One such trick is to use an old browser to try to dupe the airline into serving a simpler version of their page that is easier to scrape and manipulate. Another tactic is to use automated tools to test credentials as a precursor to a more targeted attack.

This quarter the network detected a series of transactions from old Chrome browsers as well as high-velocity transactions from a single device that were detected and were presented with targeted friction.

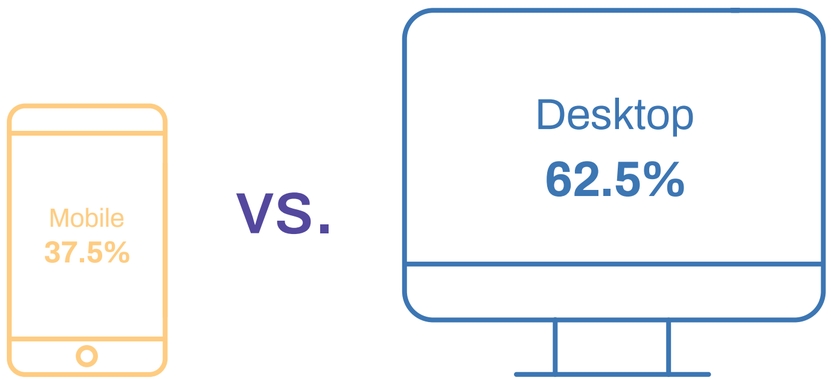


Mobile vs. Desktop Attack Patterns

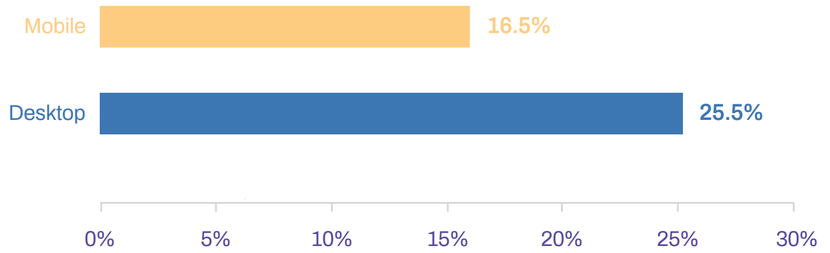
The mobile share of transactions grew 20% compared to the previous quarter with every third transaction now originating from mobile devices. Overall attack levels for mobile grew compared to last quarter, however, the growth of attacks for web transactions was higher, showing that this is still where fraudsters concentrate their efforts. Attacks on mobile transactions accounted for 33% of all automated fraud attempts and 20% of all human-driven attacks.

The proportion of traffic coming from mobile varies by industry and use case. Over half of account registrations across industries are now mobile-driven. For social media, nearly seven in ten transactions come from mobile, and nearly half of gaming, retail and travel transactions originated from mobile. On the other hand, finance and technology platforms continue to be primarily web-driven.

Mobile vs. Web Attack Mix



Mobile vs Desktop: Attack Rate by Use Case



Conclusion

The last quarter of the year is a time when retailers and other digital businesses are under the most pressure due to elevated consumer activity. As commercial pressures around conversion rates and customer throughput are at their highest, this is when organized fraud mobilizes in force. They ramp up activity not only to try and blend in with genuine traffic, but also to take advantage of companies who shift their risk tolerance in the hope of letting through as many customers as possible.

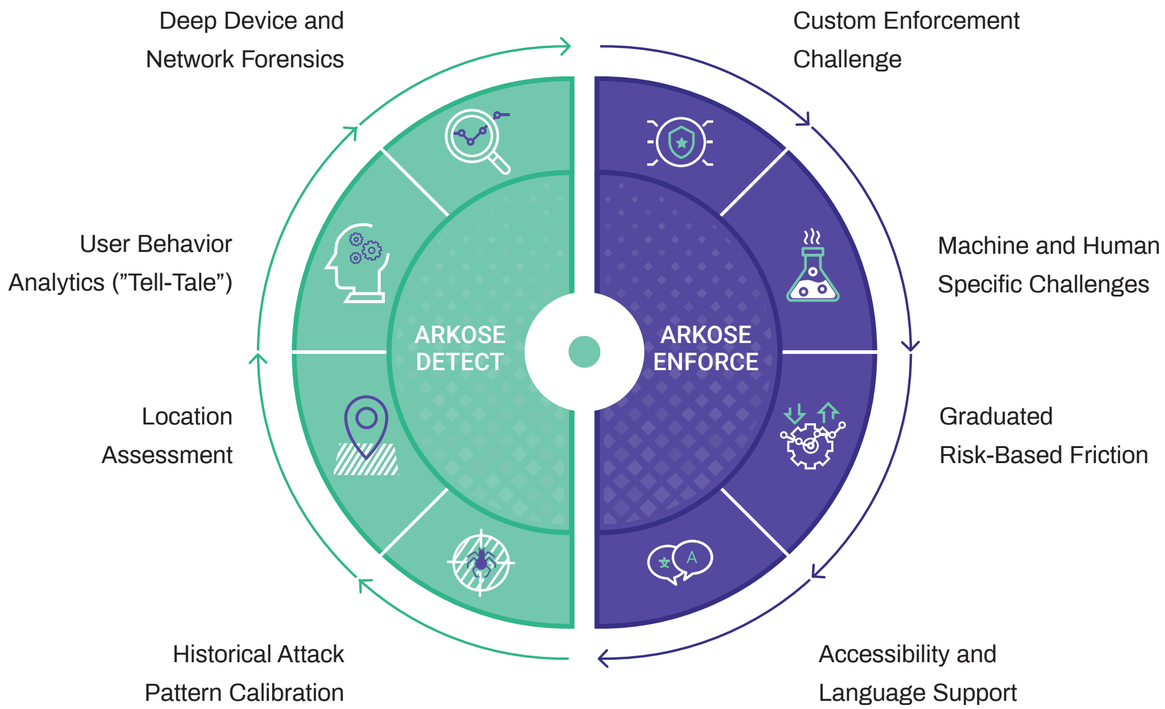
Insights from the Arkose Labs platform shows that this time of year is not only the financial highlight of the year for businesses, but also for fraudsters. The elevated rate of human-driven versus automated fraud shows that attackers are willing to invest more in their attacks, often having laid the groundwork in previous months using lower-cost automated attacks.

Both businesses and consumers increasingly recognize the need to have more accurate fraud detection procedures in place to prevent widespread abuse. The only long-term strategy to stamping out fraud is to adopt a zero-tolerance approach, which focuses on disrupting the economic drivers underpinning fraud, using a combination of risk profiling and targeted authentication challenges.

Rather than shying away from introducing friction into the customer journey, we need to rethink how this can be leveraged as a positive component. This proves to good users that they are being protected and allows businesses to accept good transactions with confidence.

Evaluating identity and intent

Arkose Labs' Fraud and Abuse Prevention Platform



Arkose Detect is Trained by Arkose Enforce Results

Glossary

Industries

- Gaming: Includes online gaming platforms.
- Social: Includes social networking and dating platforms.
- Technology platforms: Includes online technology providers like storage, access, and communication platforms.
- Retail and Travel: Includes e-commerce merchants, sharing economy and travel portals.
- FI and Fintech: Includes banks, online lenders, money transfer providers, payment platforms.

Use Cases

- New Account Origination: Account creation using stolen details.
- Logins: Testing stolen credentials, account takeover.
- Payments: Fraudulent transactions using stolen credit card details.

Telemetry and Enforcement

- Telemetry: The process that Arkose Labs' risk engine adopts to analyze customer context, reputation, and behavior to intercept bad actors.

Telemetry and Enforcement (cont.)

- Enforcement: Arkose Lab's proprietary challenge-response mechanism to remediate unrecognized transactions and feed the conclusive responses (good or bad) back to Telemetry.

Fraud Types

- Account Takeover: Breaking into a legitimate user account and taking over control using the account owner's personal information.
- API Abuse: Business-level attacks that aim to exploit API vulnerabilities in order to steal information.
- Brute Force Attack: An automated trial-and-error method used to extract passwords.
- Common Attacks: Malicious actions aimed at disrupting information networks of individuals or organizations. Eg., Distributed Denial of Service (DDoS), Phishing, SQL injection, Malware.
- Denial of Inventory: Holding items from the inventory to artificially deny availability of goods/services to genuine customers.
- Fake Account: An inauthentic account that has been created using stolen details.
- Gift Card Fraud: Numerous ways of stealing money off the gift cards.

Fraud Types (cont.)

- Inventory Scalping: An automated abuse of functionality to hoard the goods/services stock without making an actual purchase.
- Payments Fraud: An illegitimate online transaction completed by a fraudster.
- Spam and Malicious Content: Unsolicited content sent over the internet to disrupt services or extract personal information.
- Search and Scraping: A technique used to harvest data and information off the websites.
- Friendly Fraud: When a customer disputes a transaction with the issuer after receiving the goods or service.

Attack Types

- Automated Attacks
- Sweatshop/Clickfarms: Employing a large group of low-paid workers to launch attacks or make fraudulent transactions.
- Single Request Attack: A technique where breached email addresses are automatically matched with the topmost common passwords to facilitate account takeover.

About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Arkose Detect, a sophisticated risk engine, with Arkose Enforce, which uses targeted step-up challenges to wear fraudsters down and diminish their ROI. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled user experience.

Sales: (800) 604-3319

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU