Arkose Labs

Fraud & Abuse Report

Q4 2019

Foreword

As we reflect on the first nine months of the year, it is clear that the impact of 2019 on digital commerce will be long-lasting. This year is shaping up to be the biggest on record for data breaches and no industry has escaped unscathed. Identities have been compromised for individuals who have applied for a credit card, ordered food through a delivery app, signed up for a movie card, bought cosmetics online, played video games or were born in the country of Ecuador.

If identity has become the currency in the digital world, then data is the fuel that powers the digital economy. The scale of this year's breaches underscores the fact that both have been compromised on multiple levels.

Individuals' online profiles can be understood through the devices they use and the unique digital footprint left across applications and IP addresses. This data is used to differentiate good user behavior from the bad, however, digital footprints are now easy to replicate. With tools that clone trusted devices and spoof residential IP addresses, it has never been easier for fraudsters to masquerade as a true consumer.

Not only do fraudsters have access to complete user identities, they have also obtained invaluable behavioral data. Having detailed information about the shopping patterns and digital habits of a victim puts the power firmly in the hands of the fraudsters.

With so much in flux, it is time for us to rethink how we most accurately differentiate between legitimate customers and fraudsters, by combining data insights with targeted friction. As the gray zone of suspicious activity flagged by fraud indicators expands, intelligent step-up can be the missing link that clarifies whether or not a good customer's digital footprint has been corrupted by fraudsters.

Kevin Gosschalk
CEO & Founder, Arkose Labs

Report Overview

The 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 July 1, 2019 to Sept. 30, 2019. These sessions, spanning account registrations, logins and payments from financial services, ecommerce, travel, social media, gaming and entertainment 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.

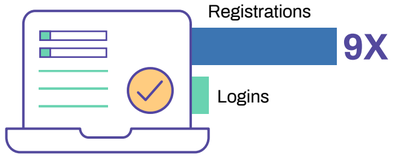
- While Arkose Labs supports multiple use cases across the customer journey, these have been broadly grouped under Account Registrations, Logins and Payments.

Top Trends: At a Glance

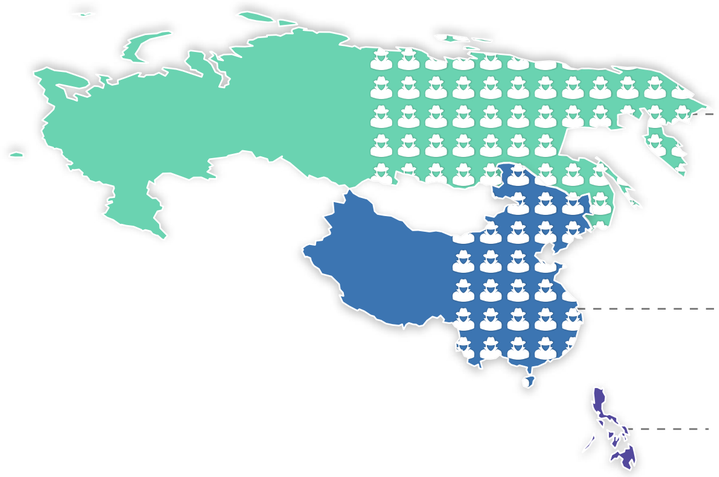
Overall attack rate
30% higher

70% higher bot-driven attacks for account registrations

Account registration **attacks on gaming doubled**

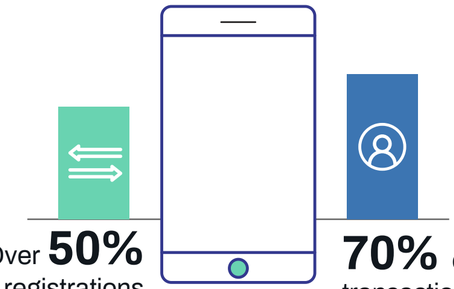


Tech registration is **9X** more likely to be attacked compared to logins



Over half of the attacks from Russia and China are human-driven

60% decline in attacks from the Philippines

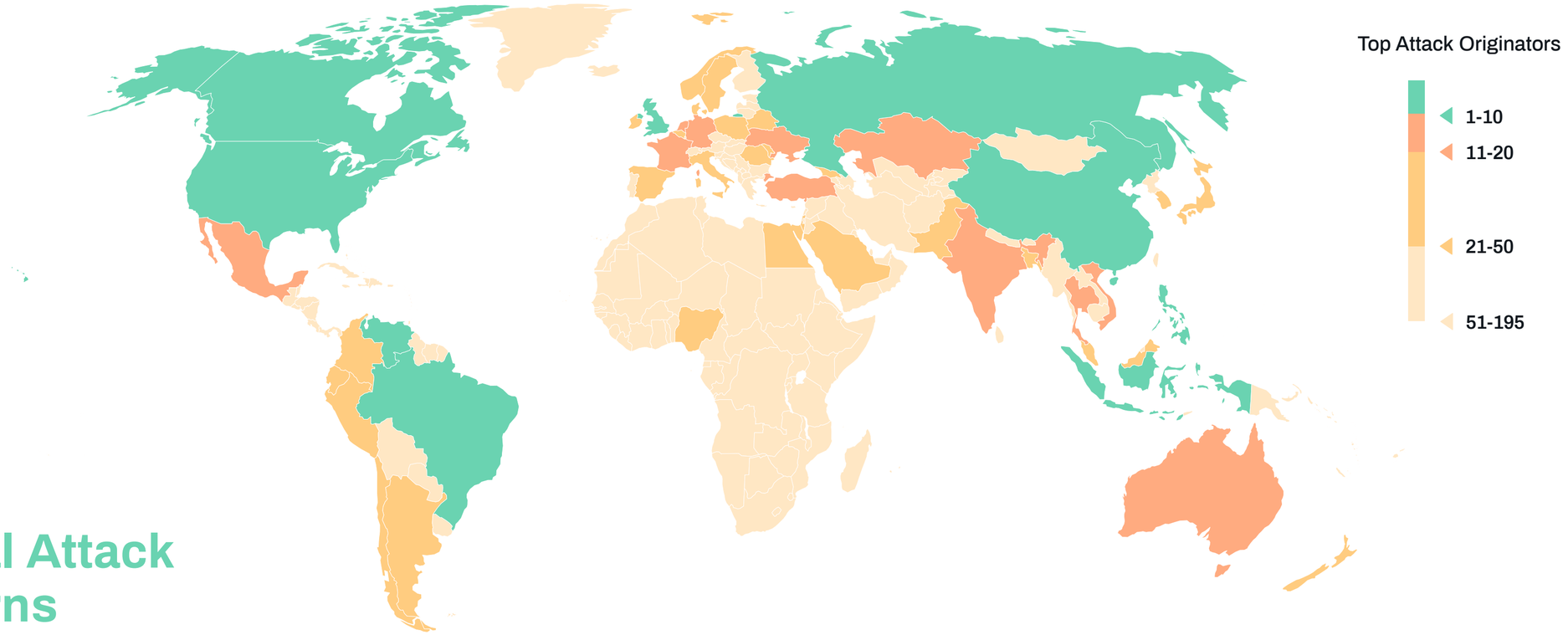


Over **50%** of all account registrations are mobile-driven

70% of social transactions are mobile-based

Report Highlights

- Arkose Labs analyzed over 1.3 billion transactions across multiple use cases and industries
- Account access (logins, reviews, updates) and account registration represent the bulk of the use cases, demonstrating the high engagement users have with their digital platforms.
- 13.7% of all sessions are attacks. These attacks range from fake account registrations, promotion abuse, account takeover, inventory scraping, spam and fake listings.
- Account registration attacks are the most attacked customer touchpoint, with every 1 in 5 account openings being malicious.
- An increase in attacks from malicious humans—both one off and organized fraud sweatshops. Nearly a third of all account registration transactions come from malicious humans.
- Over half the new account registration attacks on the technology industry are human-driven.
- Every third attack on financial services is human-driven with the most sophisticated ones coming from lone fraudsters with access to stolen identity information and the latest tools.
- The attack motivations across the globe varies driven by socio-economic differeces, access to technologiy and avaiability of cheap labor. Arkose Labs' Attack Incentive Index provides insights into how the attack patterns vary from country to country.
- Arkose Labs is witnessing the emergence of single request attacks that mimic legitimate human users and can bypass traditional bot mitigation products.



Global Attack Patterns

The global economy has never been more connected, with companies able to target and transact with customers across the globe - and global cybercrime has followed suit.
While the Arkose Labs network continues to see growth in attacks from across the globe, the appeal of cybercrime all comes down to profitability and return on investment (ROI), which can vary significantly by region. Developing economies are quickly becoming fraud hubs, spurred on by easy access to sophisticated tools, the availability of low-cost manual labor and economic incentives associated with online fraud.

The US emerged as the top attacker this quarter, with high volumes of domestic attacks on the thriving digital commerce space. US companies are also heavily targeted by cross-border attacks. The impact of recent breaches can be seen in the growth of account origination and login attacks from emerging economies.

Top 5 Attacking Countries Show Variance in Human vs Bot Attack Mix

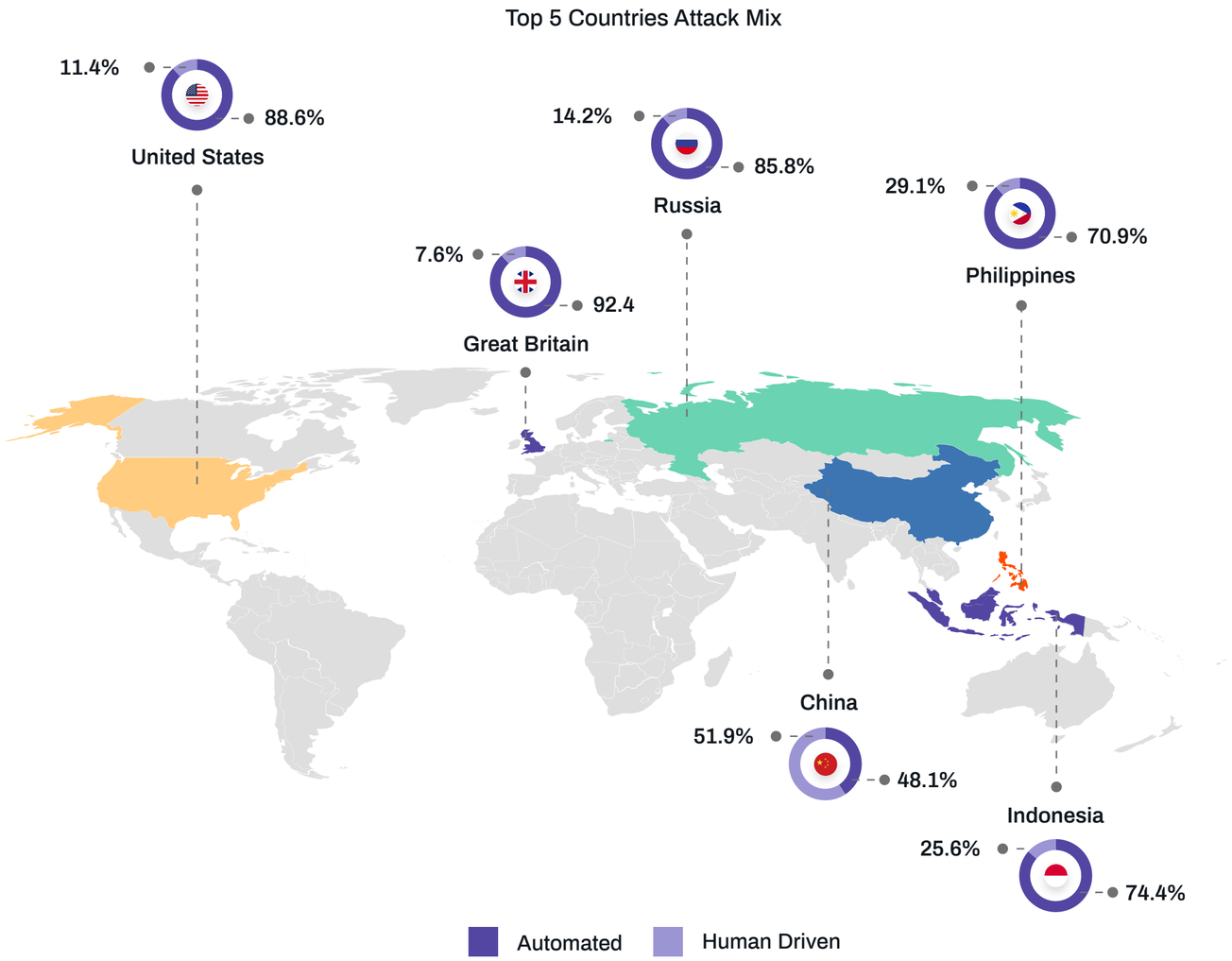
While automated attacks still represent the bulk of all attacks, the rate of human-driven attacks is growing. This is due to success rates of automated attacks declining, alongside an increased focus on identity proofing and corroboration across industries. As businesses are refining their processes towards human-centric design, the need for human presence in attacks is increasingly critical.

Depending on the use case and associated profitability, these human-driven attacks can originate from lone fraudsters or organized click farms or sweatshops.

The lone fraudsters usually target financial institutions across highly monetizable use cases whereas the sweatshops target mass scale account testing and spams, etc.

Since human-driven attacks cost more, sweatshops will often shift their focus to target other businesses once they come across resistance, due to lack of profitability. This quarter, the attacks from Philippines, Indonesia and Vietnam fell as fraudsters shifted to other countries for resources where there are lower costs, such as Venezuela and India.

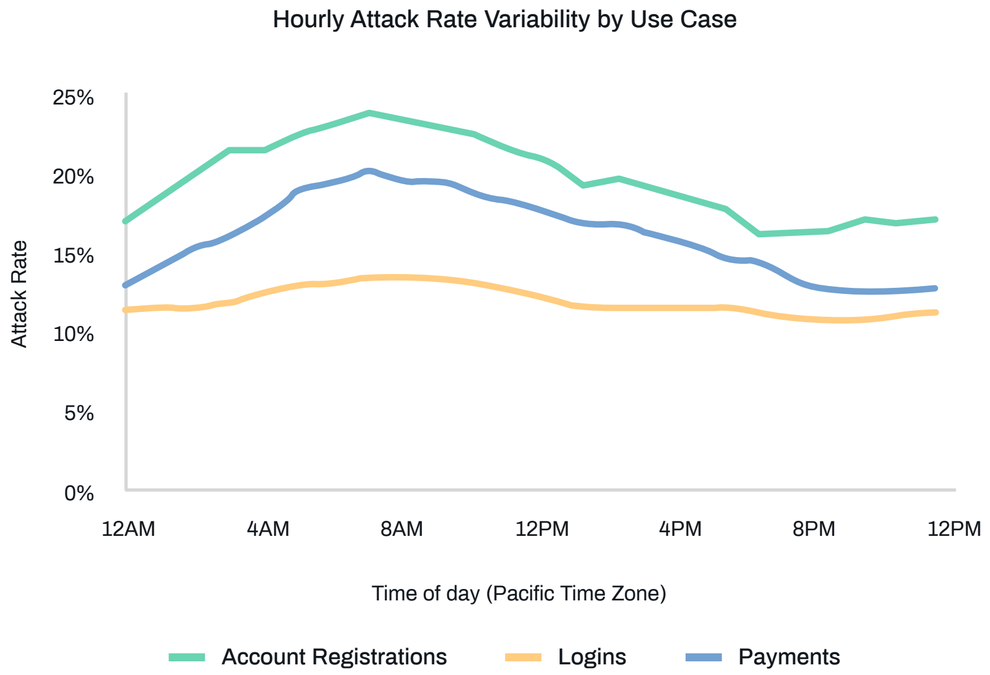
China continues to have the highest mix of human-driven attacks whereas US sees the highest overall number of attacks, both from automated bots as well as sophisticated fraudsters.



Understanding Attack Timings for Human-Driven Fraud

The variability of human-driven attacks continues to be visible, driven primarily by the ‘office hours’ the fraudsters keep and the traffic patterns of the businesses they are trying to attack.

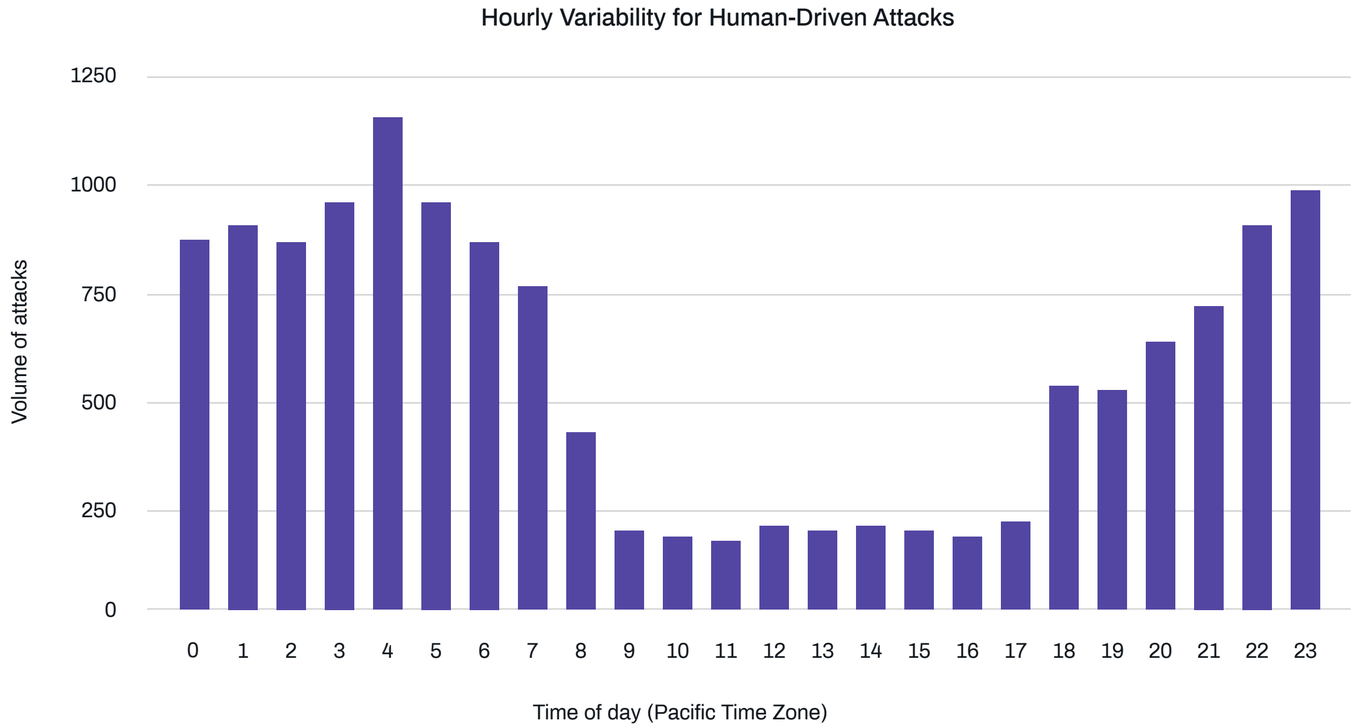
Businesses are being targeted with more intense volumes of attacks, with the peak attack level growing by 25%, and the overall peak shifting towards later in the day. Increased attack volumes can be attributed to the availability of fresh user data on the back of recent breaches as well as the increased attack rates on a few business groups.



Fraudsters' Deep Knowledge Network

The deep knowledge sharing between fraudsters also means that they are usually aware of both the tools the businesses have deployed and the times of day that they are typically updated. We saw one specific fraud group moving their attack pattern to avoid the office hours of the Arkose Labs team in an unsuccessful attempt to help avoid detection and maximize their possible return.

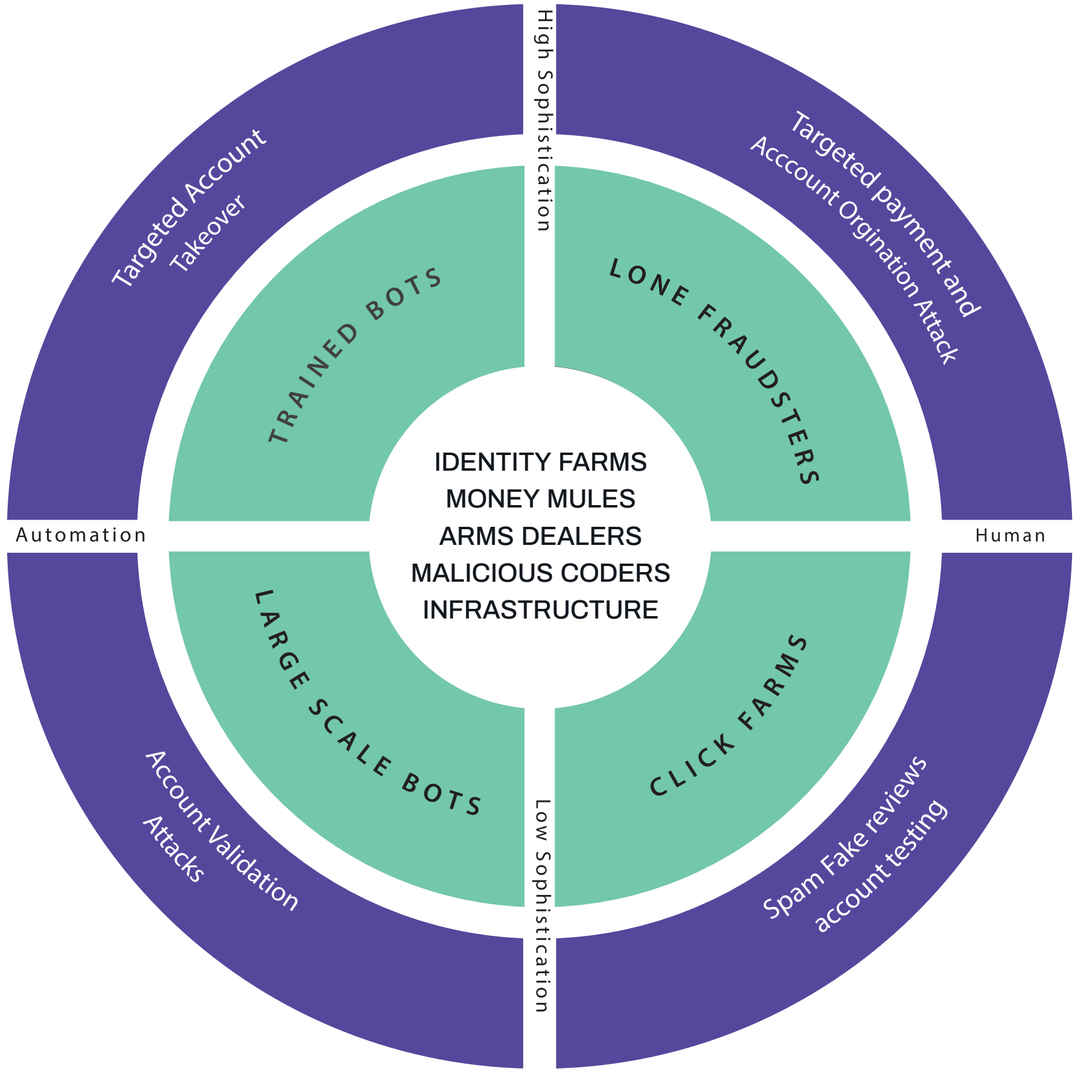
This underscores the complex, connected nature of the fraud ecosystem and the need for a fresh look at the business of fraud.



Breaking Fraudsters' Economics

Global Cybercrime Ecosystem

The growth of cybercrime has created a parallel ecosystem of businesses that support this activity and shares in the profits. An array of services have sprung up to support fraud, such as identity farms, click farms and money mule networks. This ecosystem makes it possible for large-scale, organized fraud to exist.



Attack Incentive Index - Understanding the Motivation Behind Fraud

Disparities in wages and cost of labor, differing costs of living and the comparative purchasing power of different currencies shift incentive levels among would-be fraudsters. On top of economic drivers, regions have different access to the technology needed to support sustainable cybercrime outfits.

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 ROI.

This provides insight into the effort that fraudsters are willing to expend in order to carry out attacks, which can inform strategy around authentication and friction.

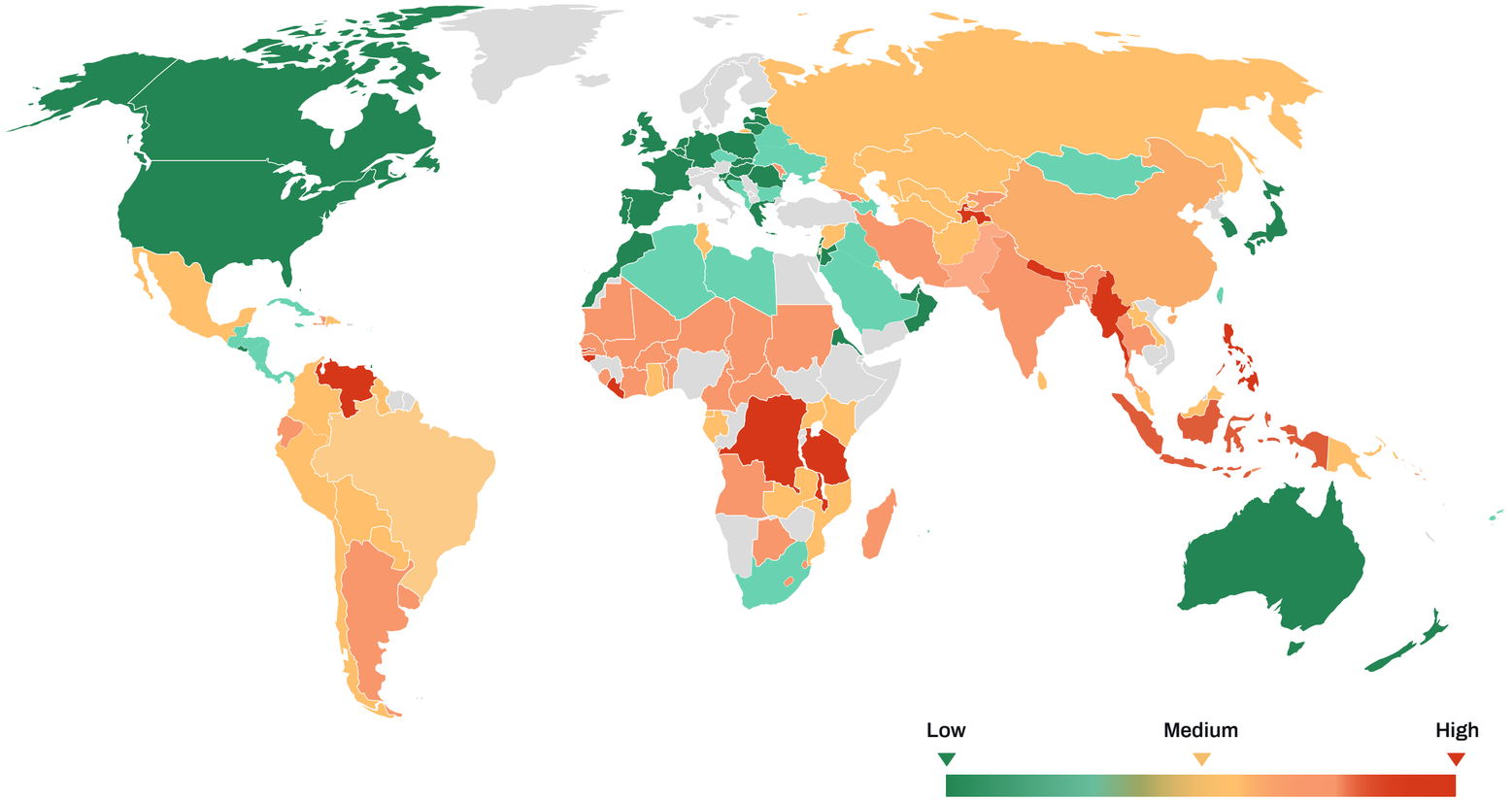
The key to addressing fraud and abuse in the long term is making friction levels for fraudsters higher than their attack incentive index, as they will abandon attack once it proves too difficult.

There will be some exceptions where fraudsters take a longer time to abandon the process, when they are looking for a blueprint for attacks which they can replicate elsewhere. Targeted friction and fraud defenses that fraudsters cannot learn to circumvent en masse are key to removing the financial incentive that is driving these individuals into cybercrime.

Attack Incentive Index - By Country

The Arkose Labs Attack Incentive Index is based on analysis of attacks seen on the Arkose Labs network, combined with global data on cost of living and wages.

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



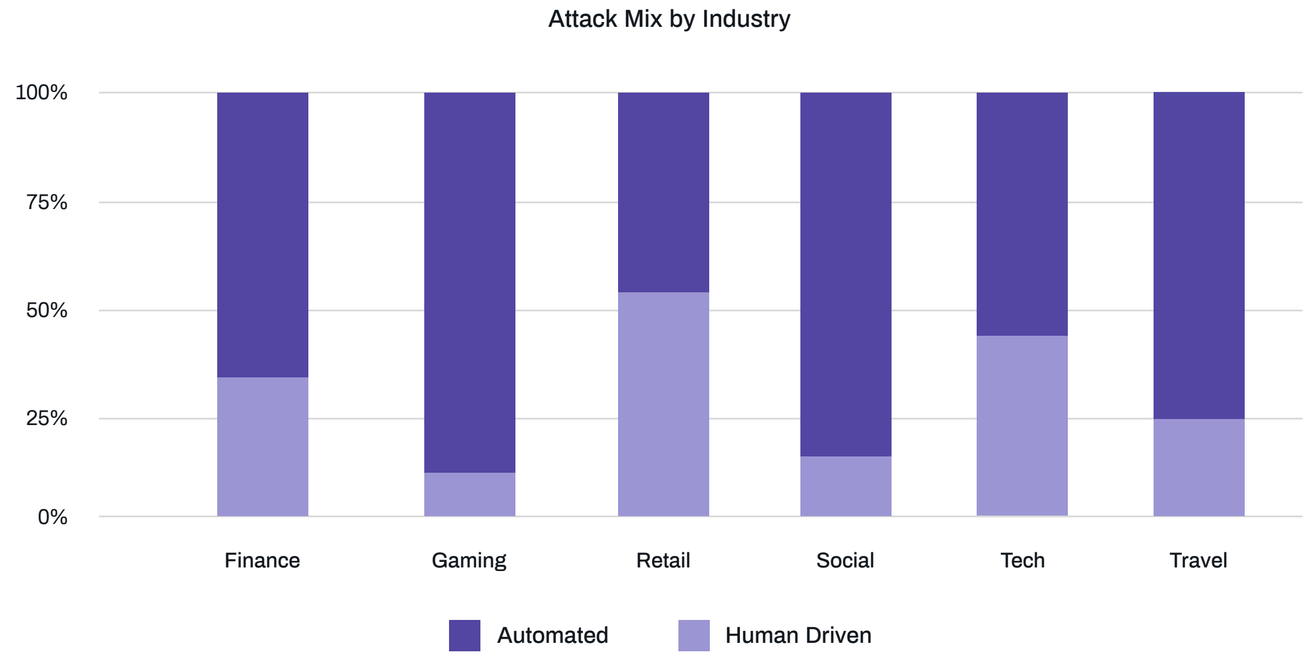
Human Driven vs. Automated Attack Mix - By Industry

Human-driven attacks are costly but sometimes necessary to pull off a good payday. The higher the potential profit, the more likely a fraudsters is to put in manual effort. As such, the mix of human-driven versus automated attacks varies by use cases and industry, with more human attacks when there is a higher potential of monetization.

For both a lone fraudster or an organized sweatshop, the key is to find the right mix of human effort and bots. Often automated attacks are the precursor to a sophisticated human-driven attack.

As businesses' defenses move towards a more human-centric design, the need for human interaction is becoming increasingly important for certain use cases. This quarter, nearly every 1 in 5 attacks were human-driven representing a 33% increase over previous quarter.

The biggest increase in human-driven attacks was seen in the gaming industry, targeting increased user activity over school holidays and new games releases. The retail industry has the highest levels of automated attacks that try to profit from the prioritization of order acceptance rates over fraud controls that potentially introduce friction.

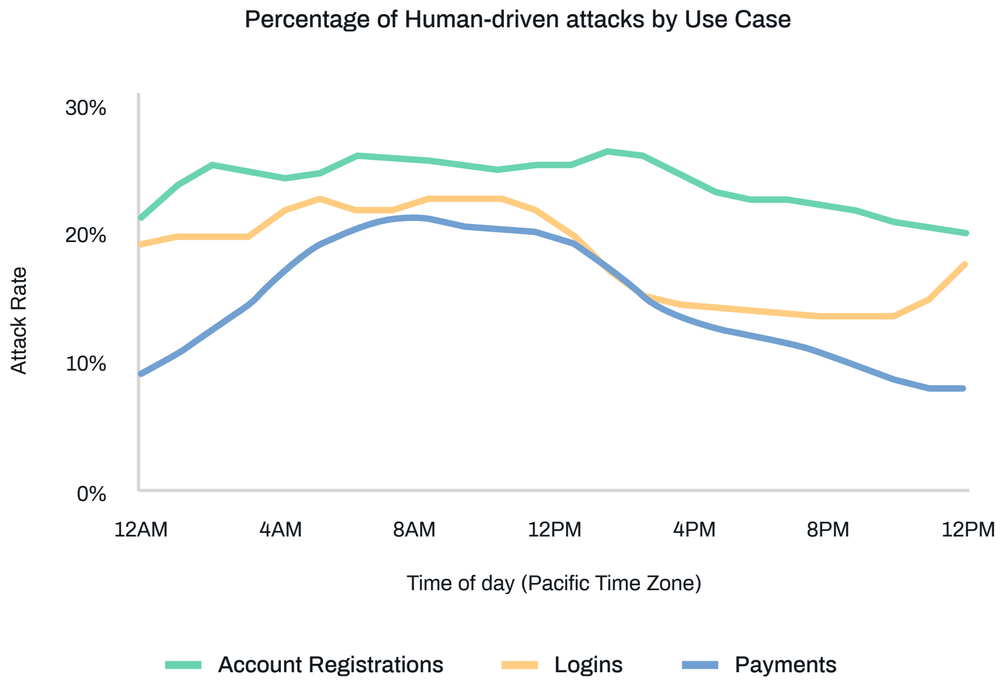


Human-Driven vs Automated Attack Mix - By Use Case

As with the previous quarter, human-driven attacks are highest for account registrations, primarily because of the interactive nature of this consumer touchpoint.

However, as more and more businesses are requiring accounts for accessing services or making a purchase, the focus on account takeover is growing. This can be seen in the higher human-driven attack mix and variability in volumes throughout the day.

The biggest variability in attack mix during the day is for payment transactions, driven by the nature of the industries they are targeting, such as ecommerce. Fraudsters target times of the day when there is higher traffic in an attempt to blend in with genuine user activity and attack volumes are often consistent with the daily variability in transaction volumes for that use case.



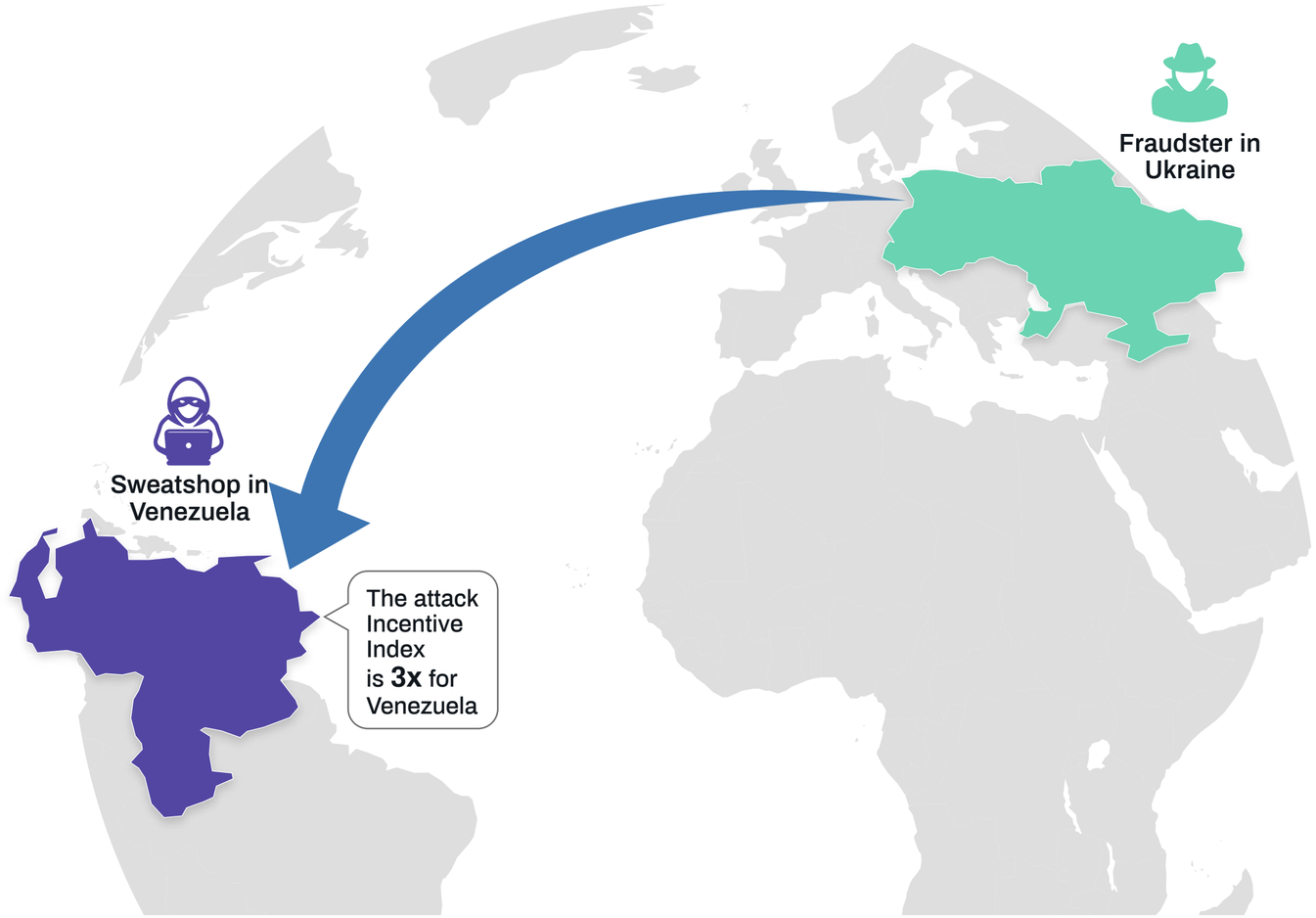
Cybercrime Sweatshops as a Business

Human-driven attacks can be divided into two main groups - the sophisticated fraudsters and the mass-scale sweatshops. For lone fraudsters, the key is achieving scale through tools and outsourced resources whereas for the sweatshop, the objective is to complete low-effort tasks as quickly as possible using a less-skilled workforce.

As such, these sweatshops are usually involved in low-value, high- volume activities such as fake reviews, spam, and fake account creations on tech and gaming sites. The more highly-skilled fraudsters focus on high-monetization activities, such as large-value purchases, applying for financial credit or running a complex in-game scam.

Due to global knowledge-sharing among fraudsters, businesses are facing a connected fraud chain wherein sophisticated fraudsters are relying on sweatshops to carry out preparation activity for a larger cybercrime attack.

The Attack Incentive Index is a good predictor of how the fraud ecosystem operates. This quarter, the network identified an attack wherein a fraudsters in Ukraine has outsourced the validation attacks to a sweatshop in Venezuela. With an incentive multiplier of 3X compared to Ukraine, Venezuela becomes the perfect “outsourcing destination”.



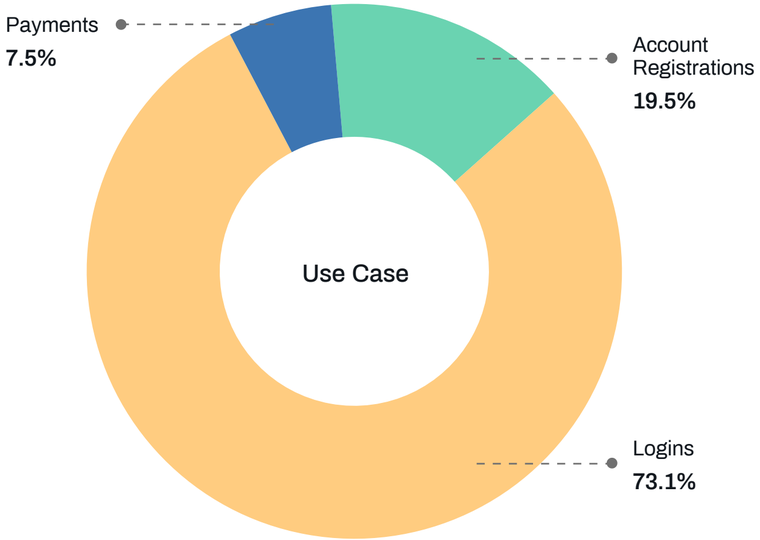
Fraud and Abuse - By Use Case

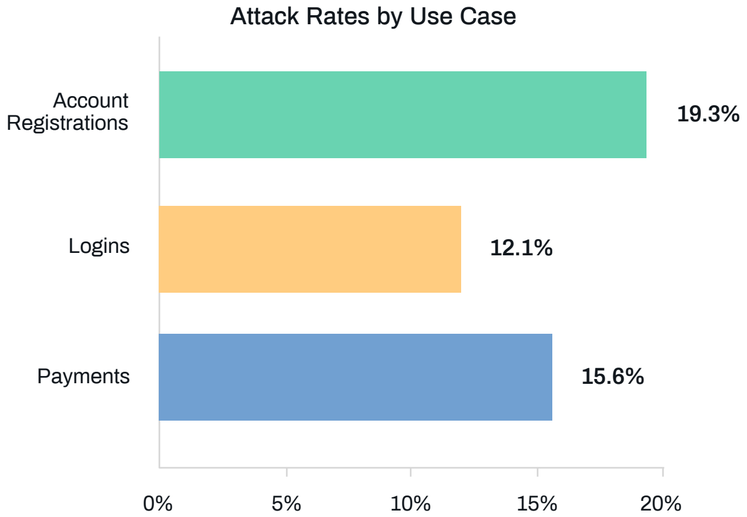
The Arkose Labs platform works with businesses across the entire customer journey. For these businesses, there are multiple touchpoints that can be grouped under account creation, login, and payments. On the back of recent breaches, the overall attack rate rose 30% compared to the previous quarter, primarily driven by an increase in fake account registrations and fraudulent payments.

Logins continue to be the biggest use case as digital-first customers and constitute nearly 3 out of every 4 digital sessions. Increased attacks on logins underscore the value of gaining access to users' account.

Digital account registration is quickly becoming the identity testing mechanism for fraudsters. This is evident in the sharp increase in account creation attacks. Bot-driven account registration attacks grew by 70% this quarter, and even when they do not succeed, these attempts can provide valuable insights into the existence of an account with the business. This information is then used for a more sophisticated account takeover attack.

While attacks on payments and account registrations increased sharply this quarter, the human-driven attack mix increased drastically for logins. As fraudsters find it increasingly difficult to launch successful account takeover attacks using automated tools, they are required to shift their focus to human-led attacks.

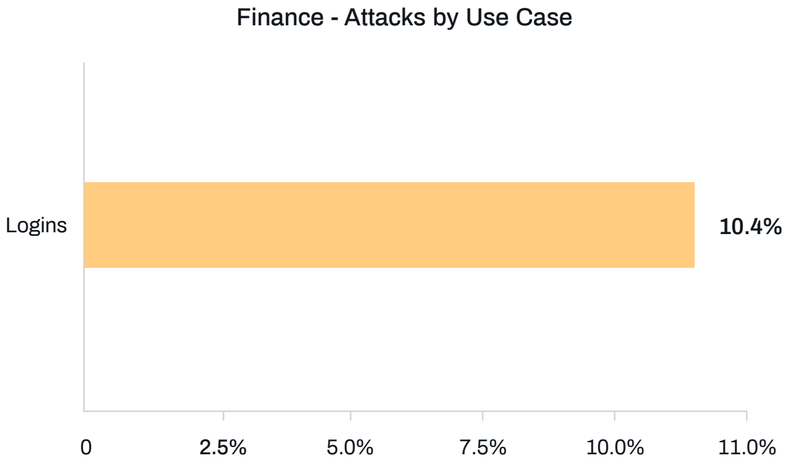


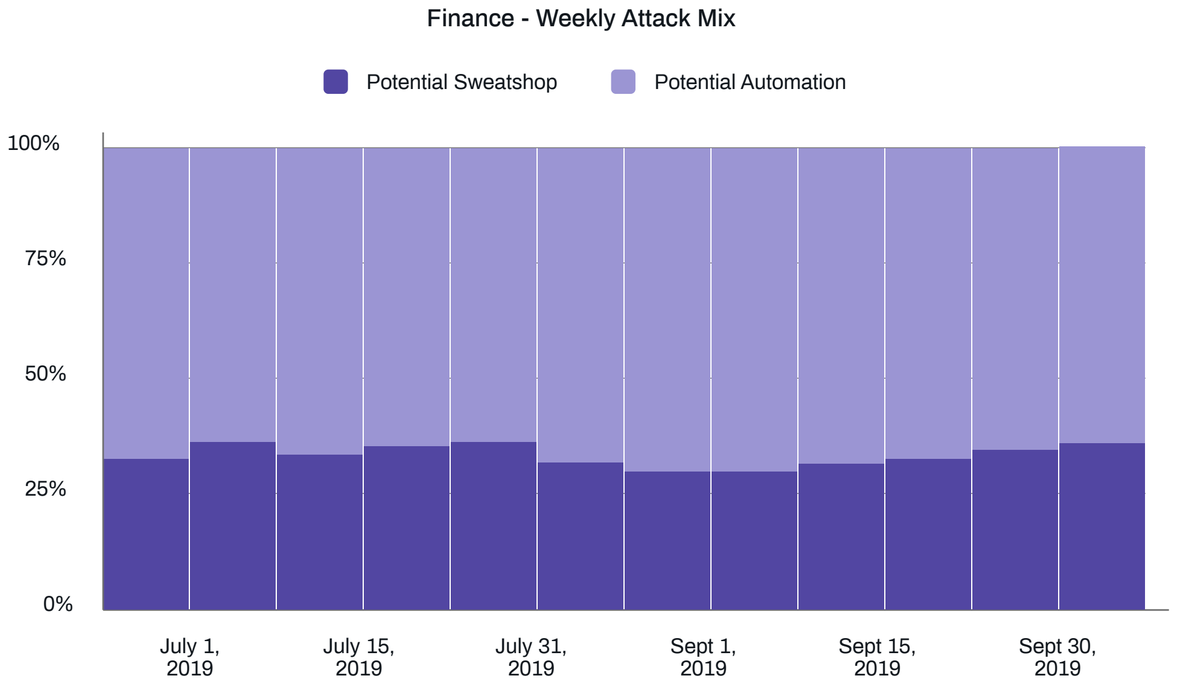


Finance and FinTech Transaction Analysis

Technology advancements have had a major impact industry-wide for the financial services sector. From major digital transformation programs within traditional banks, the emergence of mobile-only challenger banks, and the rise of online lenders, remittance platforms and cryptocurrency exchanges, the face of finance has fundamentally changed in recent years.

The effects of major disruption within banking and fintech is visible in the evolving nature of fraud targeting the sector. This quarter, overall attack levels within finance were up 15%, with the biggest growth coming from human-driven attacks. Arkose Lab's 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.



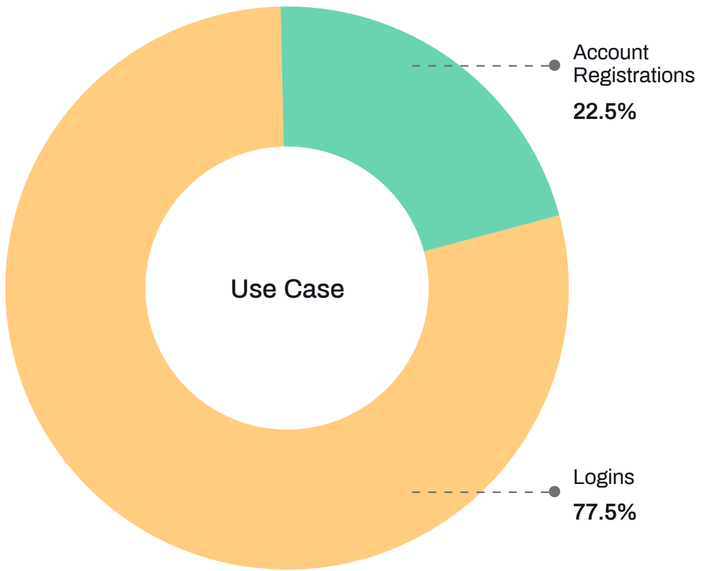


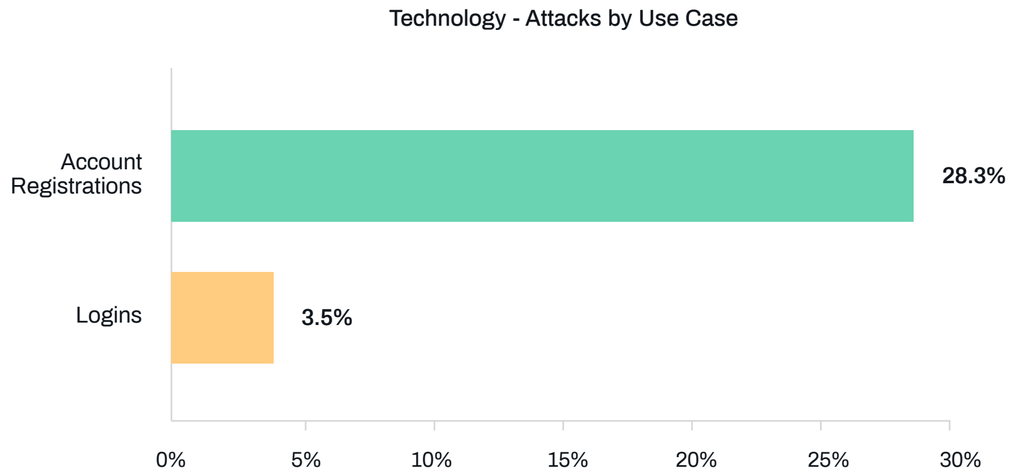
Technology Platforms - Transaction Analysis

With businesses moving to the cloud, technology has emerged as a key segment, offering vital access to distributed workforces, including communication platforms, flexible storage and office tools. Primary customer touchpoints for this segment are account registrations and logins, with payments mostly happening in the background.

These use cases are attacked by fraudsters looking to either test credentials using fake account registrations, or to scrape content and disseminate spam after gaining unauthorized account access. This segment also experiences one of the highest levels of attacks from sweatshops.

This quarter saw a huge spike in attacks on account registrations, both from automated bots and humans. Account registrations were around nine times more likely to be attacks compared to login attempts. This is because the freemium model offered by many tech companies provides the perfect outlet for fraudsters looking to either test stolen credentials or create fake accounts in order to access services.





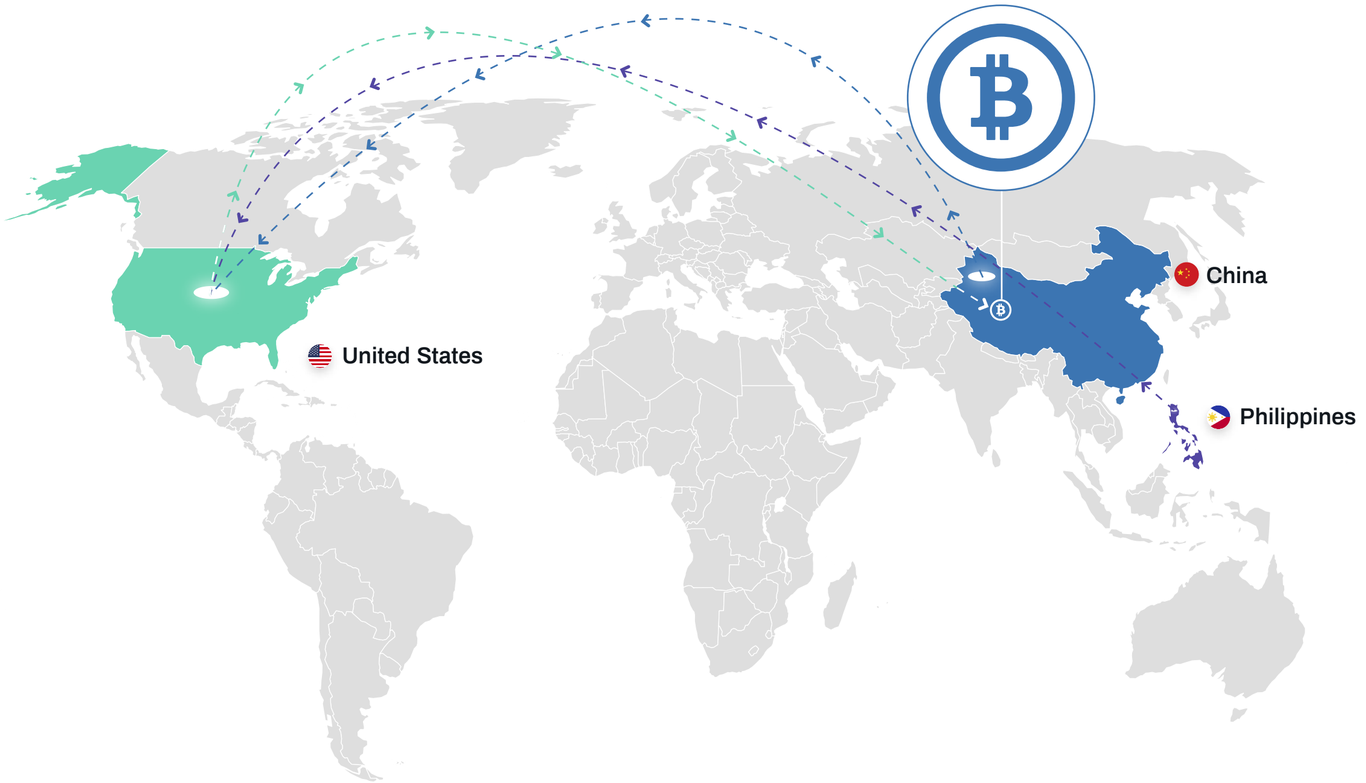
Tech Case Study: Fraud as a Means and Not the End

The Arkose Labs network detected malicious activity on a technology platform where fraudulent accounts were set up in order to abuse promotions and free trials giving access to cloud infrastructure. This was a means to an end, with the ultimate objective of using free server time to mine for Bitcoin.

The high monetization potential associated with Bitcoin led to elevated levels of human-driven activity. 50% of attacks on tech platforms last quarter were carried out by fraudsters and sweatshops as opposed to automated tools.

Using their knowledge about typical fraud detection methods, fraudsters based in China leveraged location spoofing to masquerade as domestic users; used sweatshop resources in South East Asia to bypass bot detection tools such as CAPTCHA; and kept attack volumes low in order to better avoid detection.

Using advanced telemetry and step-up challenges that hamper fraudsters' ability to up fake accounts, Arkose Labs were able to work with the technology platform to stamp out abuse and ensure that promotions were offered to legitimate new users only.

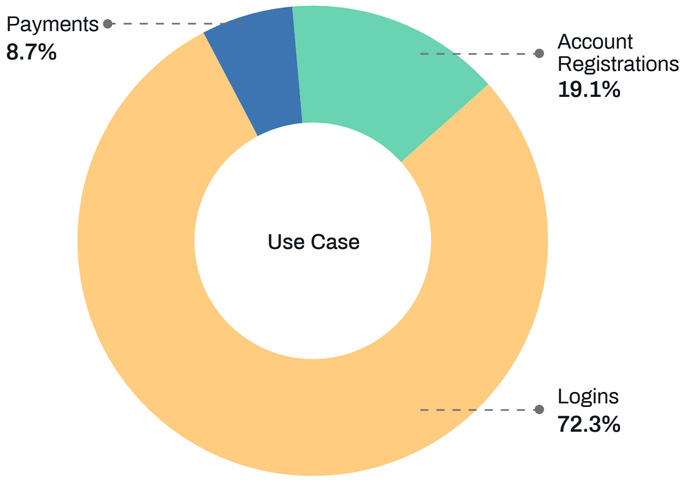


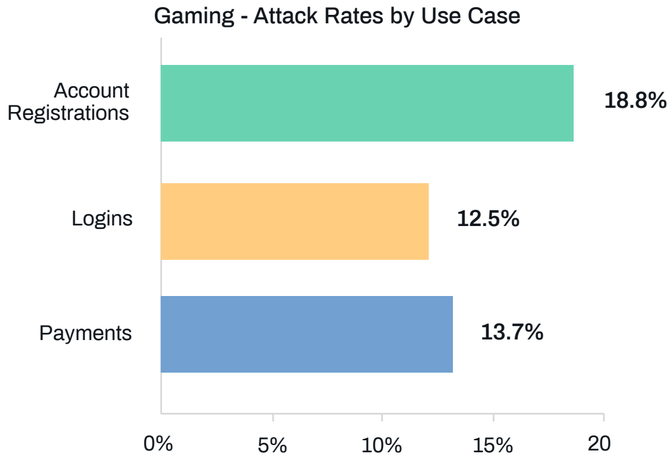
Gaming Transaction Analysis

Customer engagement for the gaming industry is one of the highest, with millions of users logging in daily to play their favorite games. Customer experience is critical in this segment, with conversion rates having a big impact on profitability, especially for in-game purchases. As the popularity of online gaming has grown, games and in-game assets have become key targets for organized cybercrime and are open to increasing levels of abuse from recreational users.

Fraudulent activity within gaming varies drastically from other industries, with unique monetization opportunities. Fraudsters can profit from stealing and selling on in-game benefits like skins, power-ups and tools; use bots to build up account profiles and sell accounts with higher levels; or target online currencies used within select games.

Some of the most sophisticated attacks seen on the Arkose Labs network are those targeting gaming segments, with some of these attack patterns later being replicated within other industries. The overall attacks levels 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

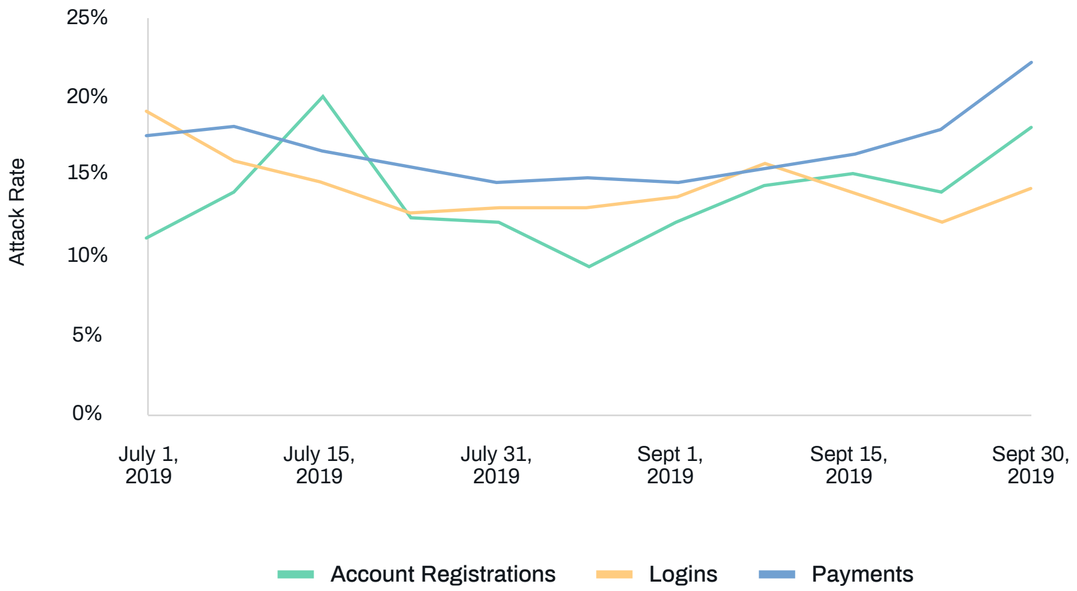
Attacks on gaming platforms are primarily driven by automation, however, certain use cases, such as in-game reviews and fake account creations, have high levels of manual attacks, due to the two-way interaction that is required.

The gaming segment sees high variability with the attack mix during the day and throughout the year. School holidays coupled with major new releases resulted in higher-than-usual traffic and elevated attack levels in Q3.

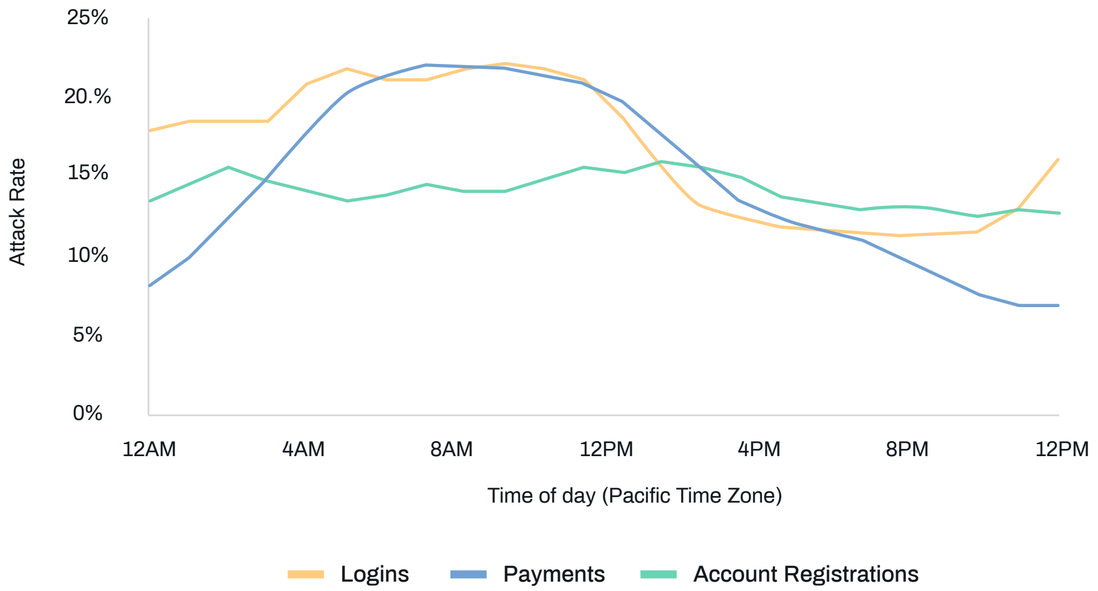
Human-driven attacks were on the rise towards the end of the quarter as different automated attempts were increasingly thwarted.

The attack mix stayed relatively consistent for account registrations but had a huge variability during the day for logins. These attacks are driven by in-game spam and abuse, while payment transactions were attacked targeting in-game currency, gift-card and auction house fraud.

Gaming - Weekly Attack Mix



Gaming - Hourly Attack Rate by Use Case



Anatomy of Gaming Fraud

Fraud is almost always about making money in the fastest and easiest possible way, and this is especially true within the gaming world. However, the common laws of fraud fighting often don't work in the same way in this sector. Effective fraud prevention complex due to a very high focus on conversion rates, the need for quick or instant decisioning, the use of real, virtual and earned in-game currencies and assets, and an elevated presence of friendly fraud.

This segment is targeted with some of the most sophisticated fraud tactics, with fraudsters coming up with increasingly inventive ways to monetize in-game interactions and target lucrative auction house transactions.

Fraudsters are aware of the data collected by traditional fraud detection systems and have access to tools that help even the most basic programmer to change and manipulate the values that are collected.

With these automated tools, the fraudsters can identify a set of values that mimic a good device and then this combination is used over and over again, once it has been proven good. This leads to traditional systems banning legitimate users as they match the attack characteristics.

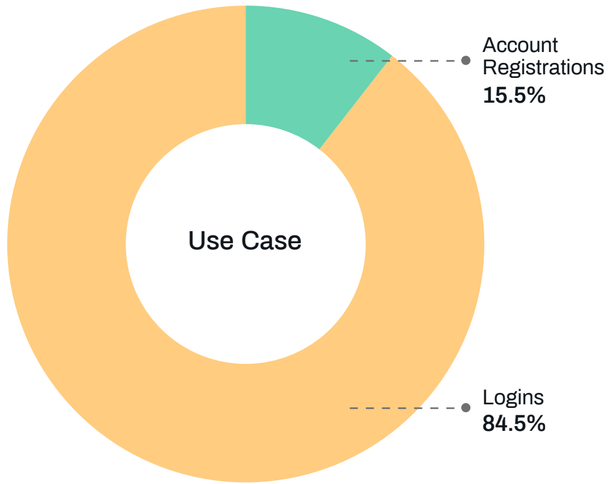
As fraud detection systems adapt to detect these attacks, fraudsters move on to new styles of attack, where the fraudsters focus on randomizing the characteristics to continue presenting as a new device or user rather than trying to find optimal values to mimic legitimate users.

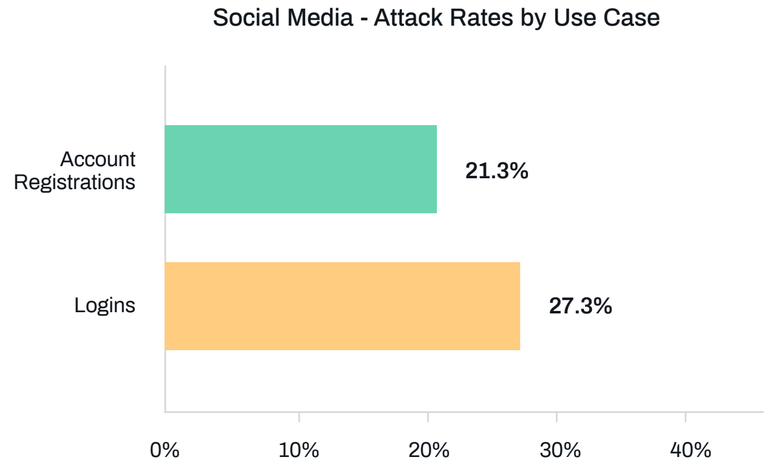
Social Media Transaction Analysis

Global popularity and high customer engagement for social media platforms makes them an attractive target for fraudsters worldwide. The evolving tactics used by fraudsters targeting this sector are clearly visible in the attack patterns for social media this quarter.

While overall attack rates fell on logins this quarter, the decline was primarily driven by the lower instance of automated attacks. Human-driven attacks on logins grew by 15% compared to last quarter as it became more cost-effective. On the other hand, fake account registration attacks were more than double the previous quarter.

Fraudsters use fake account creations as the best way to test credentials harvested from recent breaches. Social media registration attempts provide insights on the existence of accounts for users and help build accurate identity profiles by testing associations between usernames, email addresses, phone numbers and passwords. This is then followed up with a more sophisticated account takeover attacks. With password sharing across sites so common, a successful credential and password combination can unlock attacks on a user's accounts across multiple industries and websites.



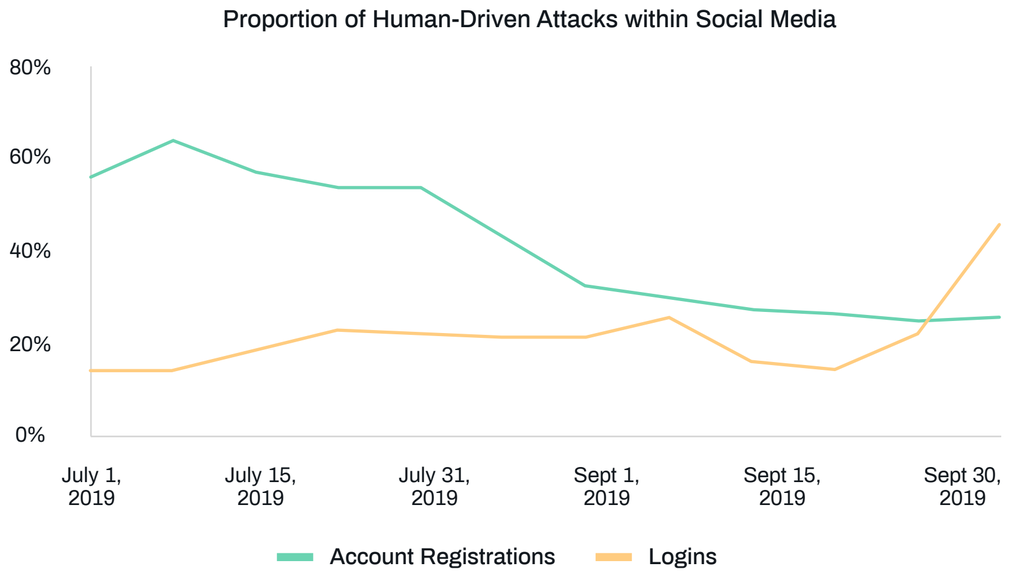


Social Media - The Connected Cybercrime Ecosystem

The attack mix for social media varied dramatically over this quarter across the use cases.

Human-driven attacks for account originations fell to ~30% from a peak of 70% in early July, whereas the mix for logins increased from 18% to nearly 50%.

This variability demonstrates how fraudsters use these two customer touchpoints interchangeably. This also highlights the fact that the fraudsters are invested in committing their fraud, regardless of the method used. As human-driven attacks on social media get blocked, they swiftly shift their focus on the next use case.



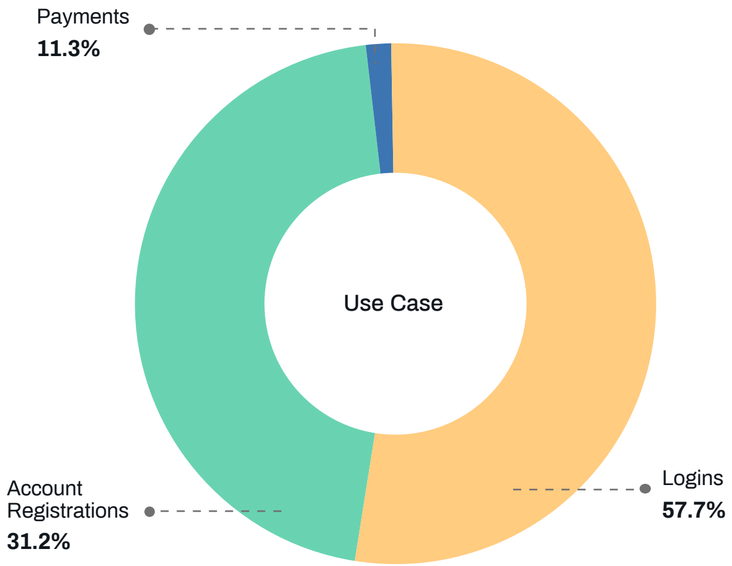
Retail and Travel - Transaction Analysis

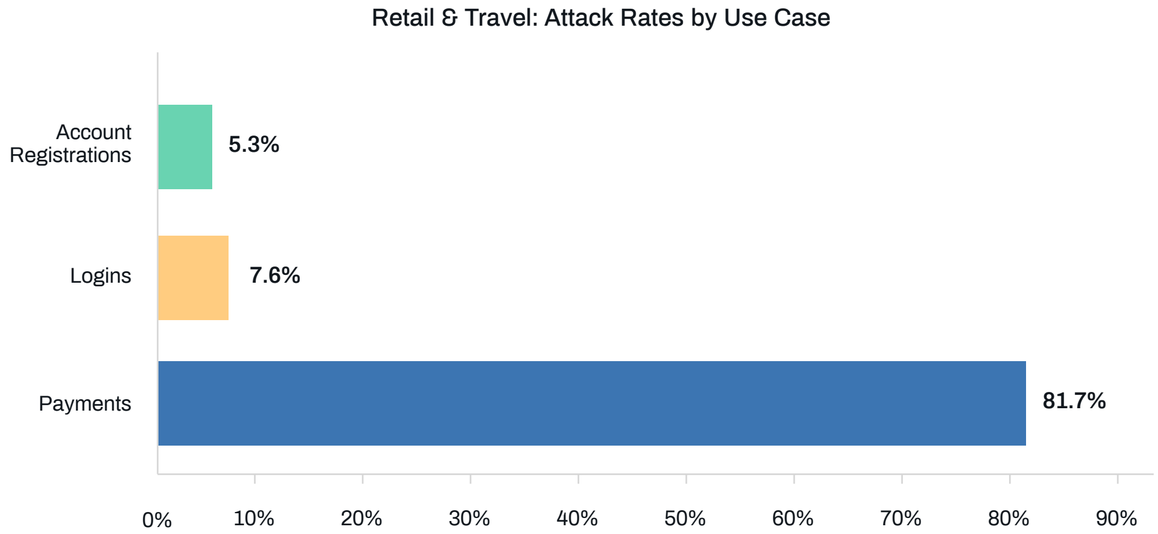
The retail and travel industries witness seasonality in their traffic with high travel volumes in summer and a busy back to school shopping season. With more and more transactions moving to the digital world, the fraud targeting these segments is rapidly evolving.

This quarter the attacks on retail segments increased sharply, primarily as more consumer data is ending up on the dark web after a succession of major data breaches this year. The bulk of these attacks were automated as fraudsters used these to test payment credentials, block inventory or scrape content.

While most ecommerce and travel companies allow potential customers to browse and sometimes even make a purchase without an account through guest checkout, companies are increasingly encouraging users to set up accounts and store payment details. As such, account takeover attacks, which increased by 30% compared to the previous quarter, are a precursor to a payment fraud.

With businesses preparing for the holiday shopping season, the increase in attack levels for retail coupled with credential testing on other sites is an indication that fraudsters are already preparing for the active holiday season to target businesses when transaction volumes are elevated.





The New Face of Retail and Travel Fraud

The ingenuity of fraudsters can be seen in the range of fraud types seen on retail and travel sites and apps.

While fraud is usually aimed leveraging fake or stolen identity credentials and payment details for immediate financial gain, that is not always the case. Fraudsters also use inventory hoarding to get access to scarce or limited edition inventory using legitimate credentials, in order to profit from the resale of popular items.

This is exacerbated by the growing popularity of the post-pay model wherein the payment is made after delivery; this gives fraudsters the window to either dispose off the excess inventory before making a payment; or else they can return the item back and not be charged for the item.

The growth of online marketplaces have not only transformed the ecommerce industry but have also provided an outlet for fraudsters to sell the excess inventory, as well as dupe customers through fake listings, items or reviews.

The screening process for account creation is often less thorough than for logins and payments, making this the perfect way for fraudsters to test credentials. These then result in account takeover attacks, demonstrating the need for intelligent fraud detection throughout the entire customer journey.

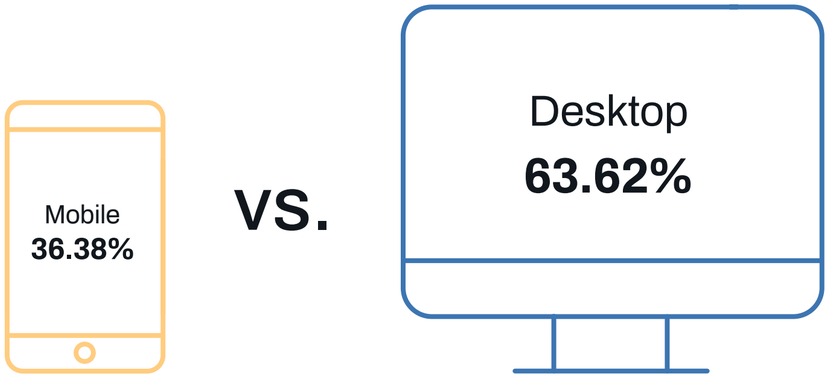
Mobile vs Desktop Trends

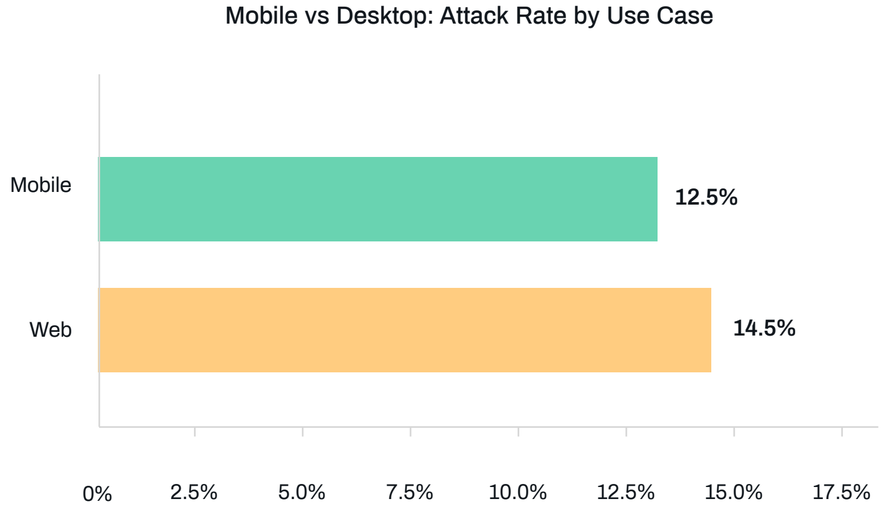
Mobile share of transactions grew by 20% compared to the previous quarter with every third transaction now originating from mobile devices.

Overall attack levels for mobile grew compared to last quarter however the growth of attacks for web transactions was higher.

The transaction mix varies by industry with nearly 7 in 10 transactions for social coming from mobile. Nearly half of gaming, retail and travel transactions originated from mobile while finance and tech continue to be primarily web driven.

At the same time, over half of account registrations across industries are now mobile-driven.





Conclusion

Fraud prevention in recent years has honed in on assessing users by their digital identity, based on the devices they use, the locations they transact from and their associated identity credentials. However, now we have moved into the next stage of the post-breach era, where there is enough data and technology at fraudsters' disposal to masquerade as individuals and spoof their devices and locations with devastating accuracy - using knowledge of current fraud controls directly against businesses they attack. As a result, organizations need to build upon data-driven fraud prevention with robust authentication steps that stop fraudsters in their tracks.

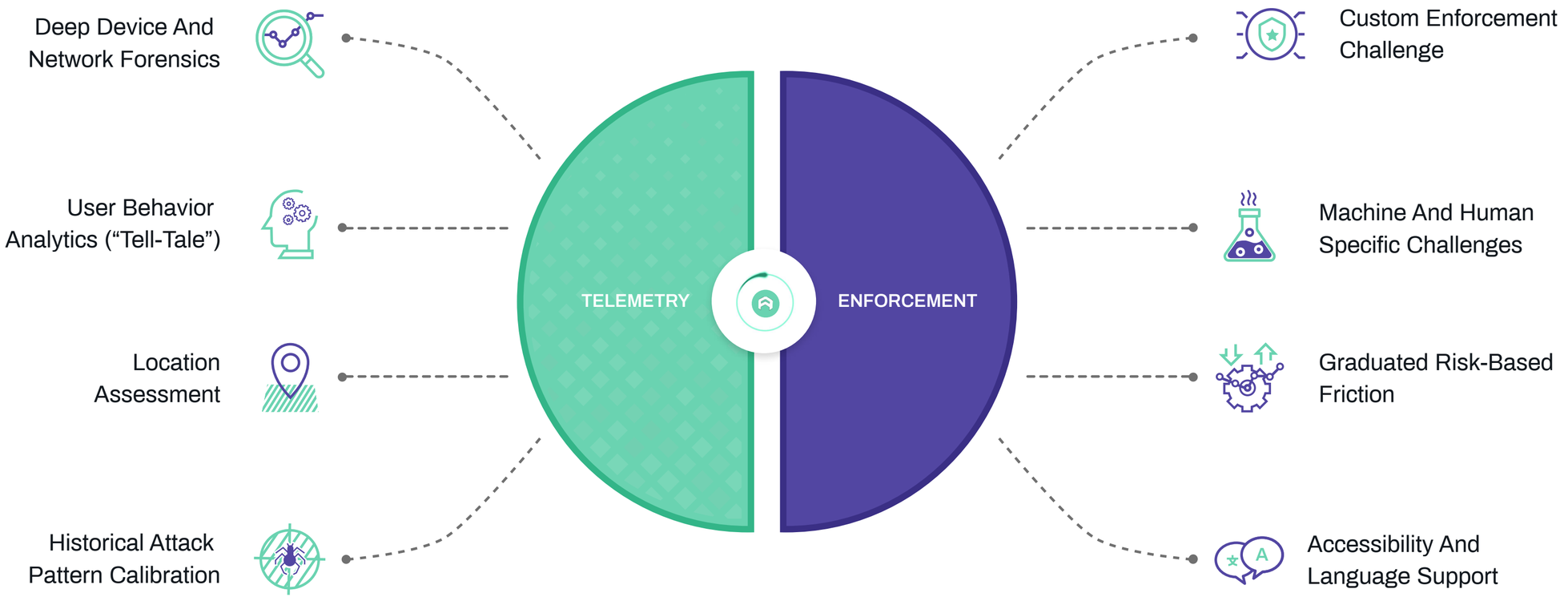
The wide range of fraudulent activity that is hitting different industries and use cases demonstrate the scale of the challenge that digital businesses face. From abuse on tech platforms which is connected to Bitcoin mining, inventory hoarding in ecommerce, and the monetization of online gaming functionalities that were not intended to have any financial value, fraudsters have become experts in creating money from nothing. They are tapping into a global cybercrime ecosystem to cut their costs and access low-cost resources, taking advantage of differences in global economic parity and differing levels on the Attack Incentive Index to carry out fraud at scale.

As we prepare for the final months of 2019, ecommerce sites are bracing themselves for the busiest holiday shopping season on record. Due to the sheer volume of breached data that has been exposed this year, we predict this to be the most significant peak in fraud and abuse that ever seen on the Arkose Labs network, with a notable spike in attacks targeting retail, travel and gaming sites.

As we prepare for this spike, we need to remain focused on how to undermine fraud in the long term, beyond tactics that deflect individual attacks. With fraudsters focused on the profit they can turn, the solution for business lies in defenses that directly attack the ROI available to fraudsters. Advanced profiling combined with targeted friction will be the most effective way to stop automated attacks, slow down sweatshop activity, and undermine the financial incentive of both lone fraudsters and organized cybercrime rings.

Evaluating identity and intent

Arkose Labs' Fraud and Abuse Defence Platform



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 ecommerce 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 recieving 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 top most common passwords to facilitate account takeover.

About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Telemetry with an Adaptive Step-Up challenge. Telemetry accurately identifies bad actors, while the Adaptive Step-Up wears them down and diminishes their ROI without adding friction for good customers. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled customer 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