Fraud & Abuse Report

Q2 2020

Foreword

Going into the new decade, none of us could have foreseen the upheaval we would witness in the first few months of 2020. The COVID-19 pandemic is a cataclysmic event that has ground whole sectors of the global economy to a halt, cast tens of millions into unemployment and upended our daily lives.

However, it has also accelerated the digital transformation of companies across the globe. As we look to protect our healthcare systems and vulnerable citizens from the devastating impact of the virus, face-to-face interactions are dwindling and more everyday activities are moving to digital channels. While there are some industries, such as travel, which have seen demand evaporate, others are grappling with huge increases in transactions.

All this flux and chaos has created almost perfect working conditions for fraudsters, with fraud levels rising on the Arkose Labs network since the onset of the crisis. Organized fraud operations have been quick to mobilize, targeting spikes in digital activity.

As businesses adjust to changing consumer behavior and fraud patterns, the conversation goes beyond protecting their own interests. The fraud fighting community needs to step up to protect individuals facing economic hardships from additional strain due to fraud and abuse, and help vulnerable new users safely navigate the world of digital commerce.

As we look to protect our healthcare systems and vulnerable citizens from the devastating impact of the virus, face-to-face interactions are dwindling and more everyday activities are moving to digital channels.

Report Methodology

The Q2 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 January to March 2020. 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 do not 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 Report: Emerging Fraud and Abuse Trends

Global rise in attacks due to COVID-19

445 million
attacks detected in Q1

44% increase in total number of attacks

Increased attack rates across use cases

49% rise in payment attack rate

18% rise in new account fraud

17% increase in account takeover attempts

Changes to regional fraud hubs

20% rise in attacks levels from United States

2X attacks from Russia

3.5x attacks from Peru

Brazil now in the **top 5** attacking countries

COVID-19: A Catalyst for Fraud

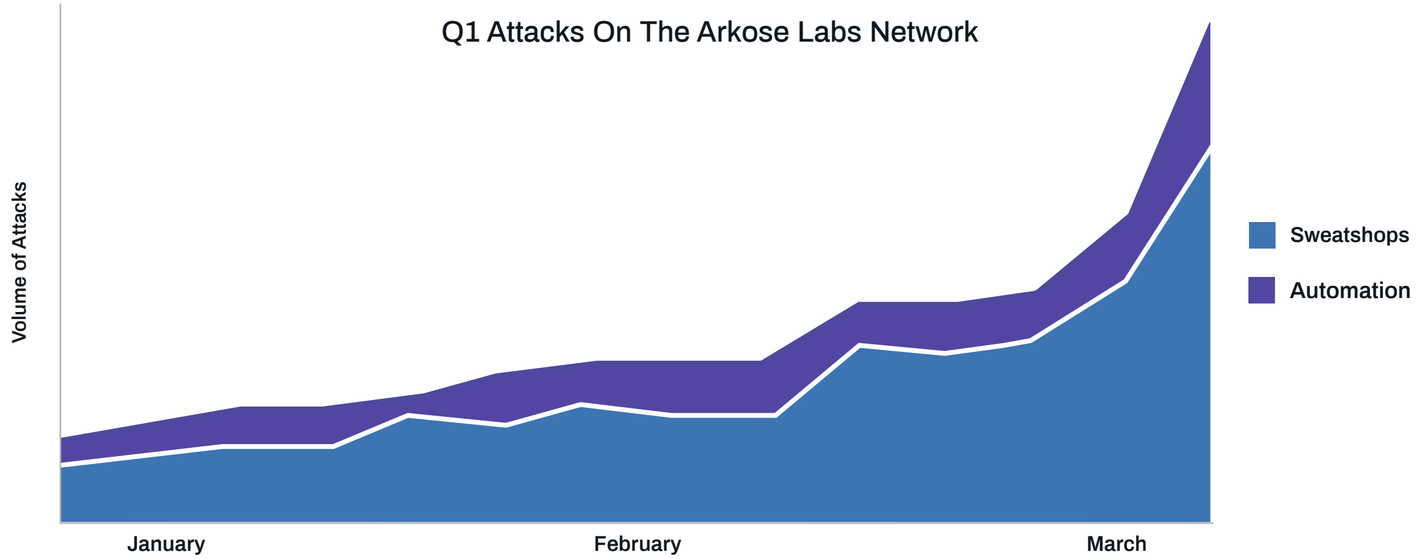
20% increase in attack rate

26.5% of all transactions are attacks

445 million attacks detected in Q1

Traditionally, Q1 is a slightly calmer period for fraud, following the digital boom of the holiday period in Q4. However, COVID-19 is upending seasonal norms. The Arkose Labs network saw the highest attack rate ever detected in a quarter, with 26.5% of all transactions being fraud and abuse attempts.

This was due to a sharp rise in fraud attempts at the end of the quarter, fueled by automated attacks, which can be scaled up rapidly. The data predicts that this trend will continue well into Q2.



Escalating Attacks Across Industries

Retail & Travel

2X attack rate for retail and travel.
The attack rate has doubled from 13% of transactions to 26%.
This is driven by attacks on ecommerce.

Finance & Fintech

Consistent attack rate for finance & fintech. Financial services saw the least variation in attack rate compared to the previous quarter.

Social Media

27% of social transactions are attacks.
One in four transactions on social media are attacks.

Gaming

23% rise in attack rate on gaming.
Due to increased traffic, this industry is emerging as a top target in the new COVID reality. This is primarily driven by automated attacks.

Technology Platforms

16% increase in attack rate on technology platforms. As personal and professional collaboration and communication moves online, attacks on tech platforms have risen.

Polarizing Effect of COVID-19 on Industries

COVID-19 is shaping up to be the next big impetus for digital transformation across industries. Widespread lockdowns and social distancing have increased global reliance on the digital economy.

Despite the overall rise in digital transactions, the impact across industries has been varied. Some sectors have seen a sharp increase in traffic and others have seen demand completely disappear. In the middle of the spectrum are the businesses that are having to quickly pivot to move revenue-generating activity online.

Top 5 Predictions for the New COVID-19 Digital Economy

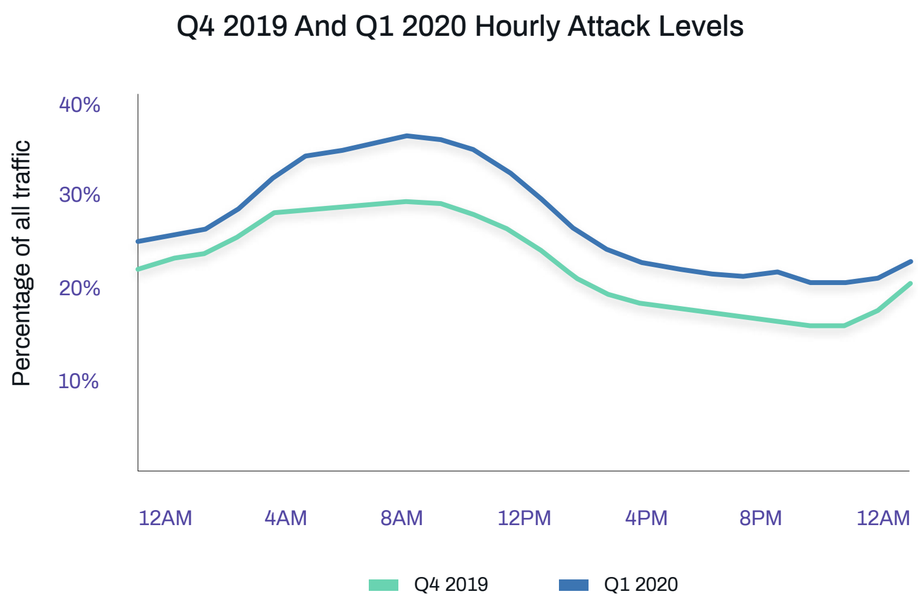
01 **Continued, dramatic rise in attacks** as fraudsters take advantage of economic uncertainty and new individuals are pushed into cybercrime due to high unemployment.

02 **Automation to drive the initial rise in fraud** as low-skill fraudsters who are new to the game take advantage of online tutorials and user-friendly, inexpensive fraud toolkits.

03 **Wider pool of sweatshop labor** available, with a move away from traditional fraud hubs to a distributed model of 'guns for hire' across the globe.

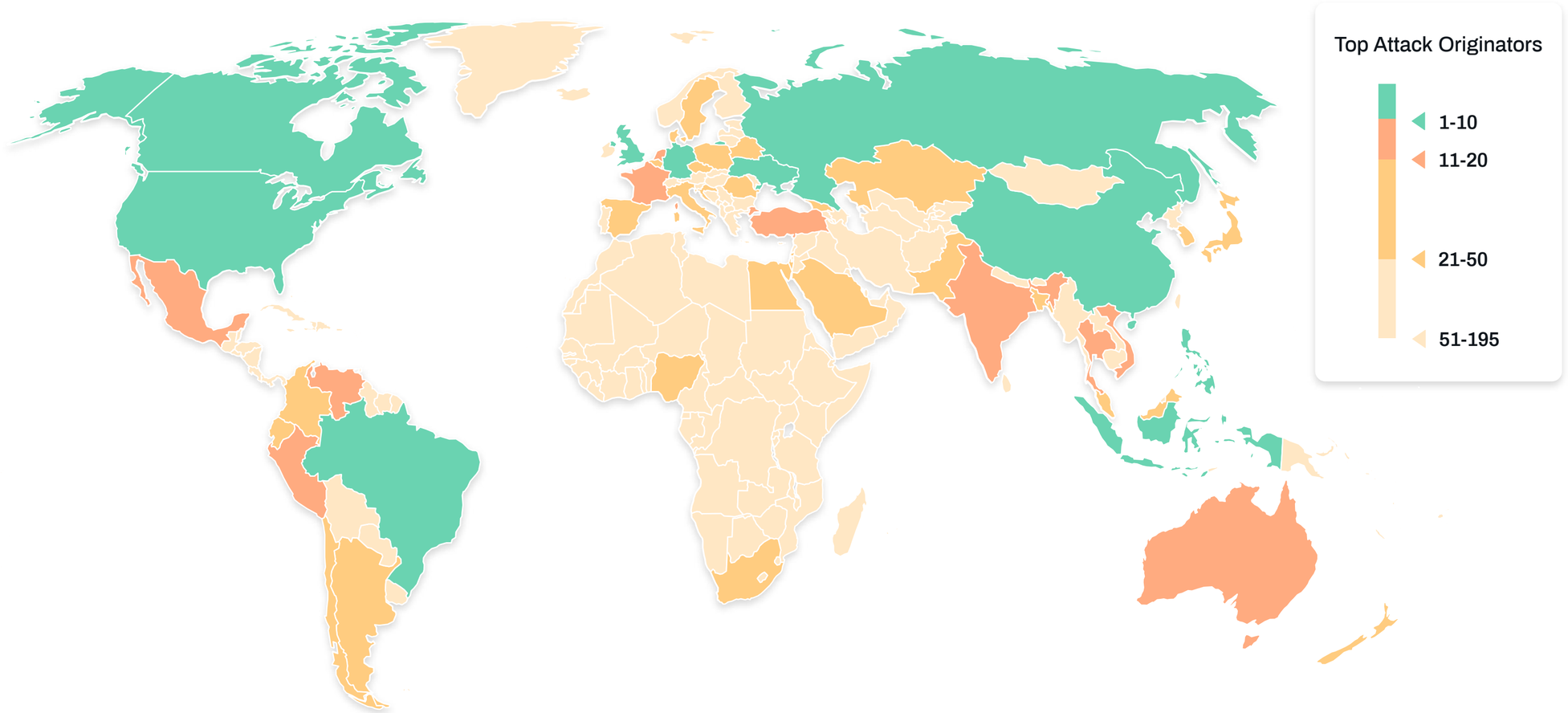
04 **New attack vectors emerge** as opportunistic fraudsters widen their reach during the pandemic, for example attacking video communication platforms.

05 **Exploitation of vulnerable individuals** with a spike in social engineering and phishing scams targeting newcomers to the digital economy.



Global Attack Patterns

Arkose Labs saw a shift in global attack patterns, with a sharp increase in attacks from established economies like the United States, Germany, the United Kingdom and Canada. As more individuals take to cybercrime in times of economic uncertainty, the total number of attacks grew by 44% compared to the previous quarter. The attack mix shifted towards a higher proportion of automated versus human-driven fraud.

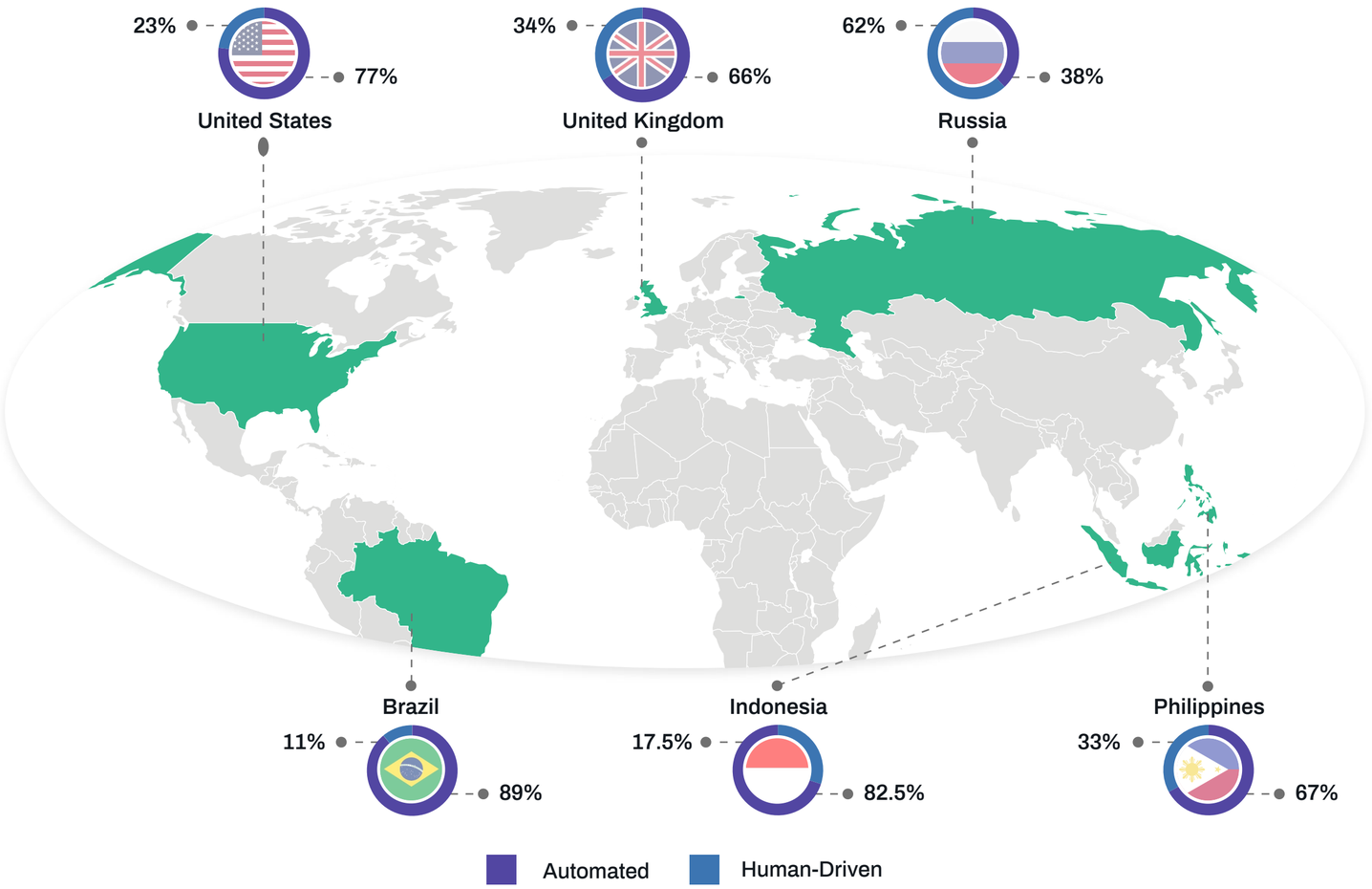


Global Fraud Hubs

The US emerged as the top originator of attacks, with a 20% rise in attacks levels. This increase in attacks was primarily fueled by automated attacks. This uptick in fraudulent activity from the US meant that it overtook the Philippines as the top attacker, although attack volumes remained consistent for this South East Asian fraud hotspot.

Attack volumes from Russia doubled and this country had the highest proportion of human-driven attacks in the top attacking countries, with 62% of all attacks being executed by humans. Brazil and Indonesia also featured in the top 6 attacking countries, with automated attacks making up the bulk of fraud attempts from these locations.

Top Attack Originators and Attack Mix



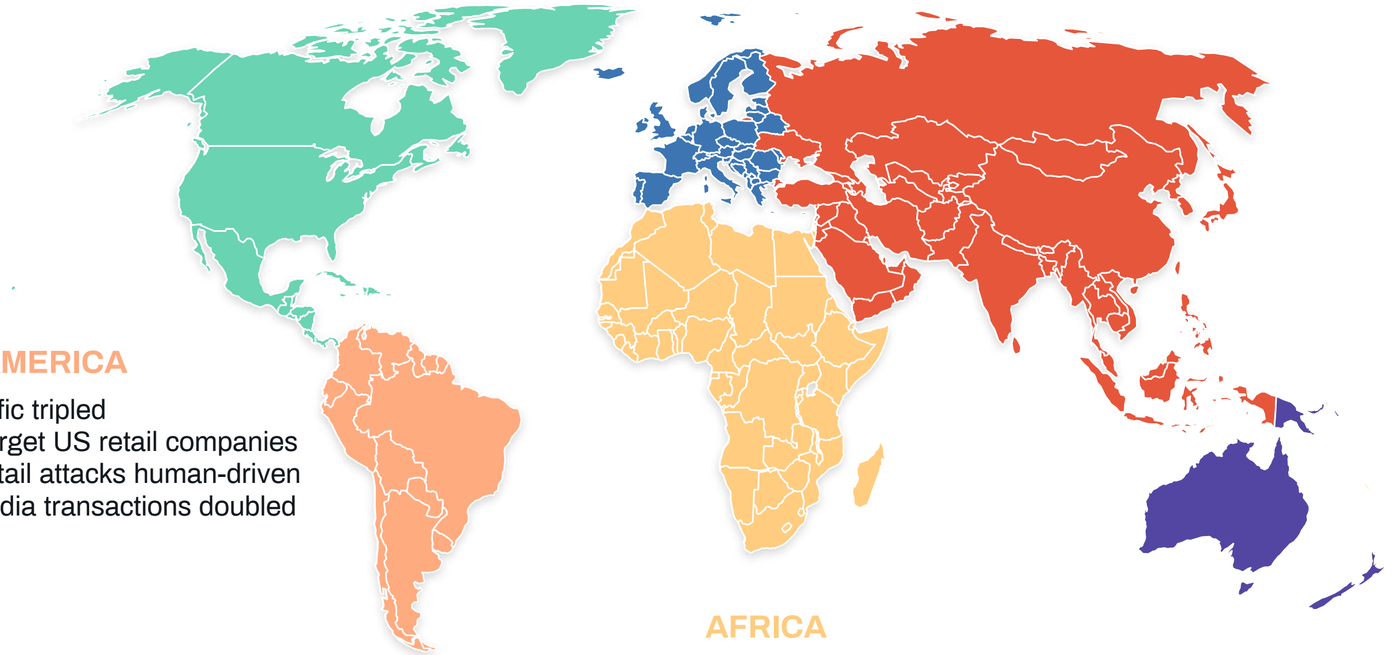
Regional Transaction and Fraud Trends

NORTH AMERICA

- High human-driven attack mix targeting social (46%)
- Spike in purchases of household items, office supplies, etc.
- 21% increase in gaming transactions
- 30% growth in travel before sharp decline at end of quarter

EUROPE

- 50% decline in travel due to COVID-19
- Lowest proportion of human-driven attacks
- 83% of attacks are automated
- Finance traffic doubled
- Strong fluctuation in online dating traffic



ASIA

- Decline in transactions across finance, retail and tech
- 40% increase in gaming traffic

SOUTH AMERICA

- Retail traffic tripled
- Attacks target US retail companies
- 80% of retail attacks human-driven
- Social media transactions doubled

OCEANIA

- Major spike in retail traffic
- 35% attack rate for tech
- 53% of tech attacks human-driven
- 26% increase in finance traffic

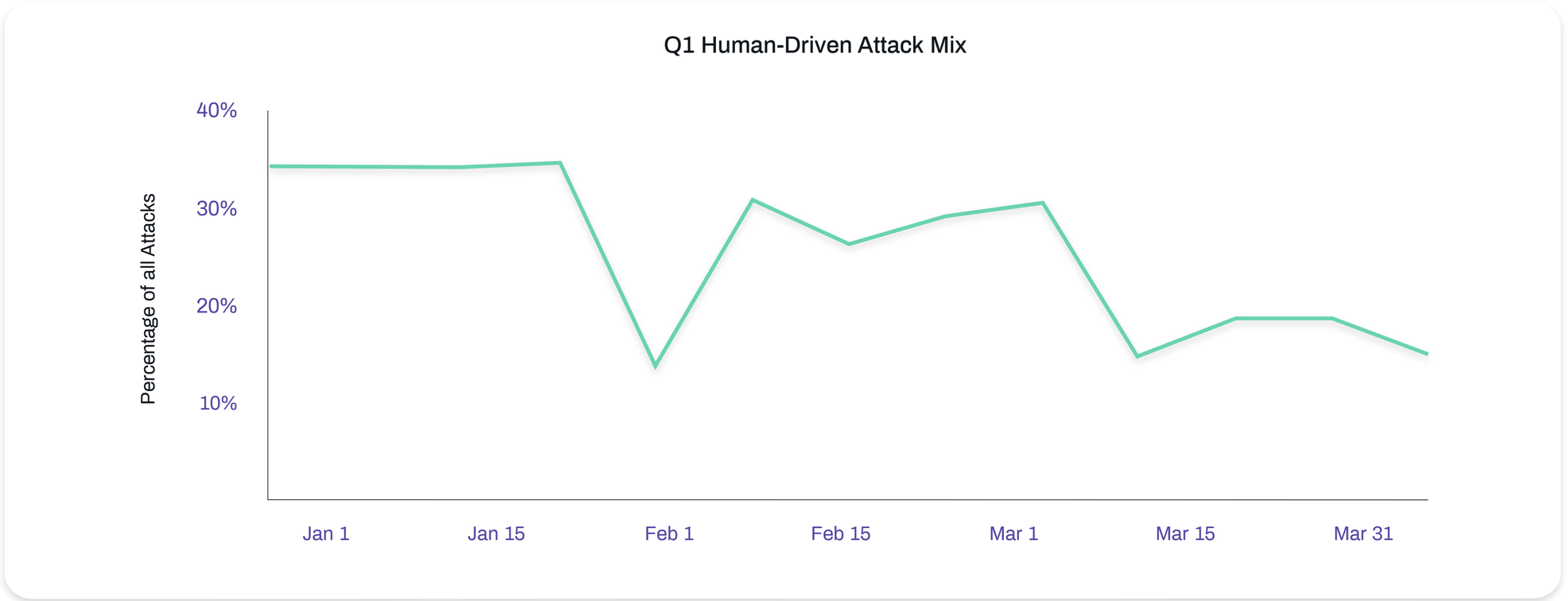
AFRICA

- One in five retail & travel attacks originates from Africa
- Spike in retail and social traffic

The Shifting Sands of Sweatshop Attacks

This quarter saw a decline in the proportion of attacks coming from sweatshops, as fraudsters ramped up automated attacks in response to COVID-19 turmoil. The overall number of human-driven attacks did increase over the quarter, however.

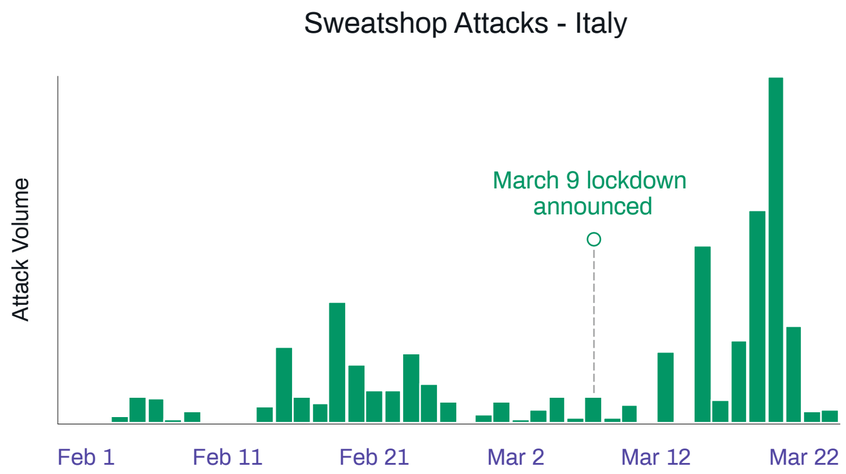
The sharp decline in the proportion of sweatshop-driven attacks in the first half of the quarter can be attributed to early lockdowns in traditional fraud hubs within Asia. As the rest of the world moved remote, so did human fraud resources. The quarter saw a move towards a distributed model, with pockets of sweatshop activity cropping up in new regions.



Fraud - A Fallback Career in Times of Economic Crisis

Localized data from countries in strict COVID-19 lockdowns show particularly interesting attack patterns. Italy and Peru both displayed pronounced spikes in sweatshop-driven activity immediately after restrictions were announced. This pattern was evident in several other countries experiencing lockdowns and closures.

Individuals who are unable to earn money in their normal way are being actively recruited by members of the cybercrime ecosystem. The speed at which attack spikes occur shows how quickly fraudsters will mobilize to take advantage of changing circumstances to maximize profits.



Fraud Trends Across Customer Touchpoints

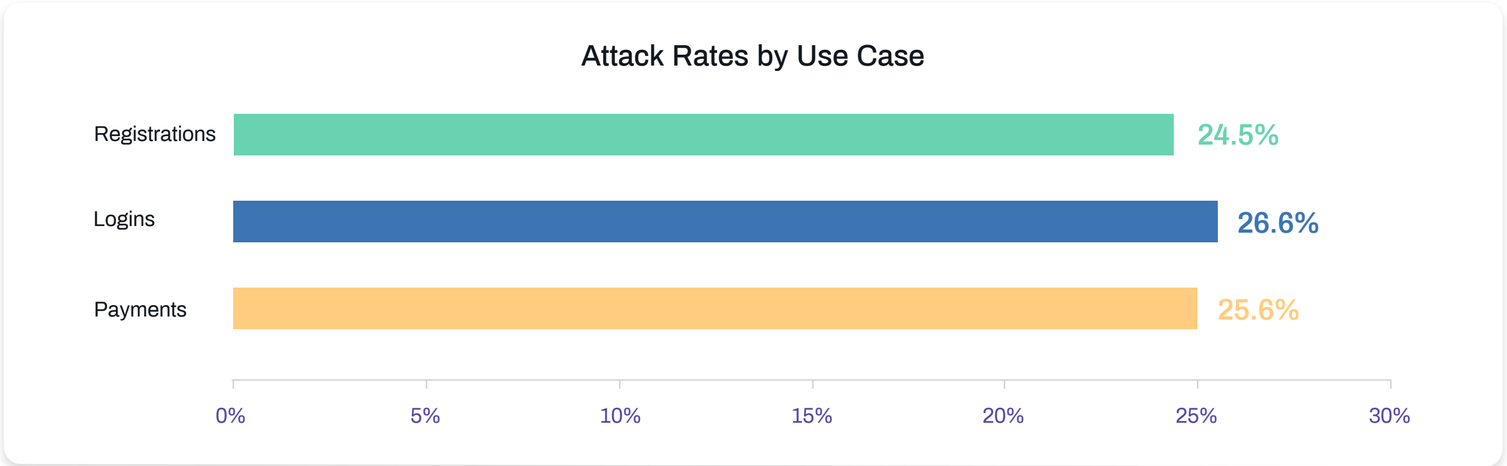
49%↑ in attack rate

17%↑ in account takeover attempts

18%↑ for new account fraud

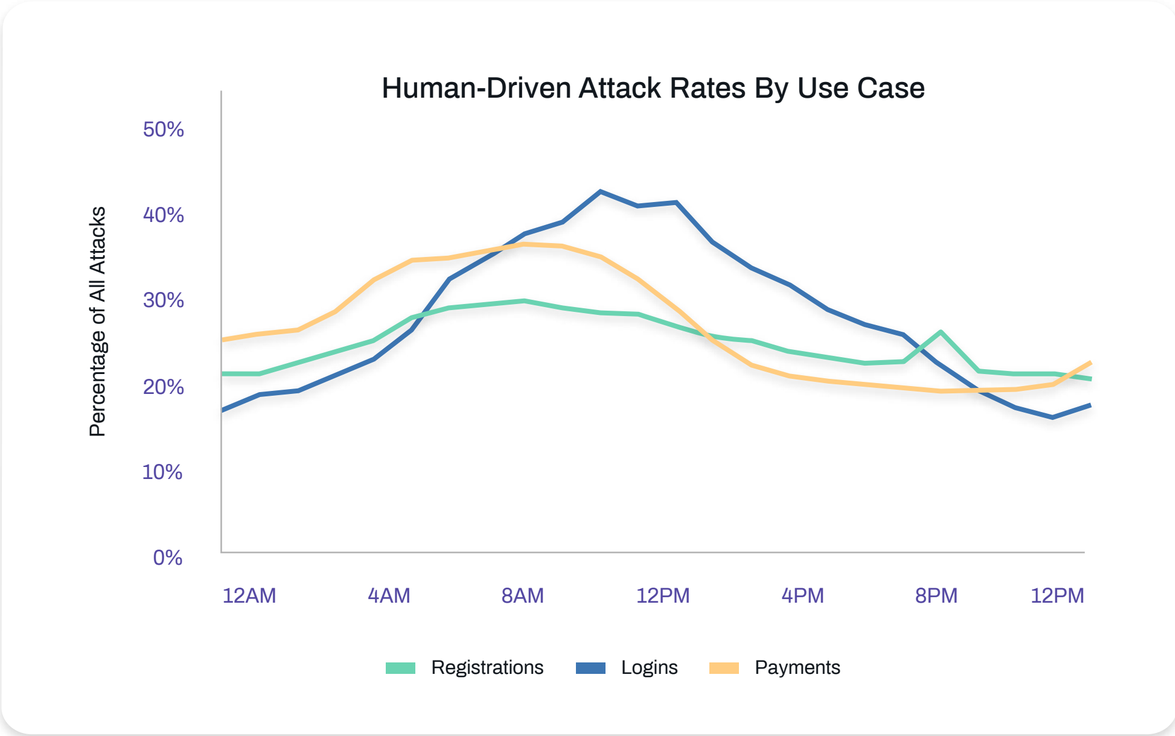
With the frenzy of fraudulent activity brought on by the COVID-19 global crisis, overall attack rates have gone up across every use case. Payment transactions show the most notable rise in attack rate and now have similar attack levels to new accounts and logins, whereas typically there has been a greater volume of attacks earlier in the customer lifecycle. Fraudsters are now operating in the perfect conditions to carry out large-scale fraud, due to:

- Cost-effective human resources to carry out attacks
- Heightened incentive levels due to economic turmoil
- Increasing digital activity across the globe
- Plentiful fresh stolen user data
- Easy access to fraud toolkits



Attack Trends Throughout the Day

Sweatshop operations are prioritizing their efforts throughout the day on payments and logins. Payment attacks, in particular, saw a clear peak in human-driven attacks in the middle of the day. Registration attacks were dominated by automation last quarter, whereas this quarter there was more consistent sweatshop-driven fake account attempts throughout the day. With individuals across the globe increasing their reliance on online services, for both work and their personal lives, sweatshops are ramping up new account fraud, hoping to blend in with the higher traffic levels.



Beyond Traditional Attack Points

Further to the standard attack points of account registration, logins and payments, perpetrators are carrying out abuse within applications, disseminating spam, writing fake reviews, and carrying out mass scraping attacks targeting identity information or sensitive commercial information. Businesses need to take an holistic approach to monitoring customer touchpoints to protect against all forms of spam and abuse.

New account fraud: Increased attack rate versus last quarter. The earlier in the lifecycle fraudsters can be detected, the better overall security of the ecosystem.

Logins: Attack rates on logins have steadily been increasing over the last four quarters, and now has the highest attack rate across the use cases.

Payment fraud: 64% of payment attacks are human-driven, which is the highest human attack mix by far.

In-game abuse: Specifically targeting online gaming companies, attack levels are comparable to login, payment, and registration attack rates. 41% of in-game abuse is human-driven.

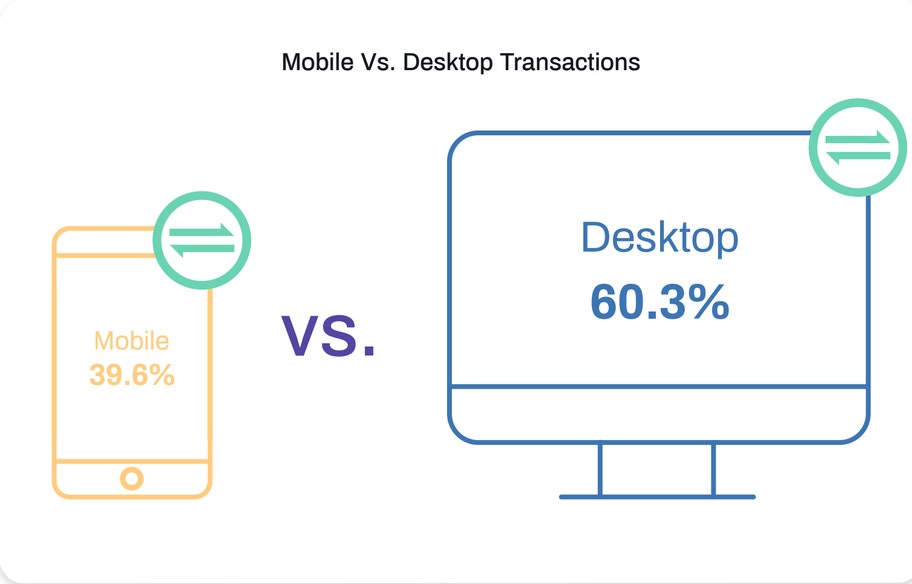
Scraping: Scraping attacks on the Arkose Labs network concentrate on select industries, such as retail and social media, and are purely driven by automated attacks.

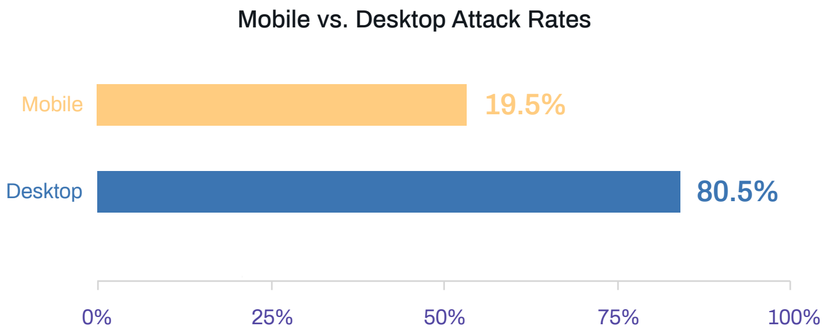
Spam and fake reviews: There has been a quarter-on-quarter rise in the volume of spam attacks and this is predicted to get more severe due to COVID-19 scams.

Mobile vs. Desktop Attack Patterns

Fraud originating from mobile devices is on the rise, however, fraudsters still concentrate more of their efforts from desktops. While 40% of overall transactions on the Arkose Labs network now originate from mobile devices, 20% of attacks are from mobile - compared to 80% from desktops. 13% of mobile transactions represent fraud and abuse attacks, while on desktop the attack rate is 35%.

Retail and social media have the highest levels of mobile engagement, whereas technology platforms are dominated by desktop interactions.





Human vs the Machine: Attack Mix by Industry

While overall attack rates grew in Q1 2020, the implications for the human versus automated attack mix varies from industry to industry as fraudsters look to maximize returns.

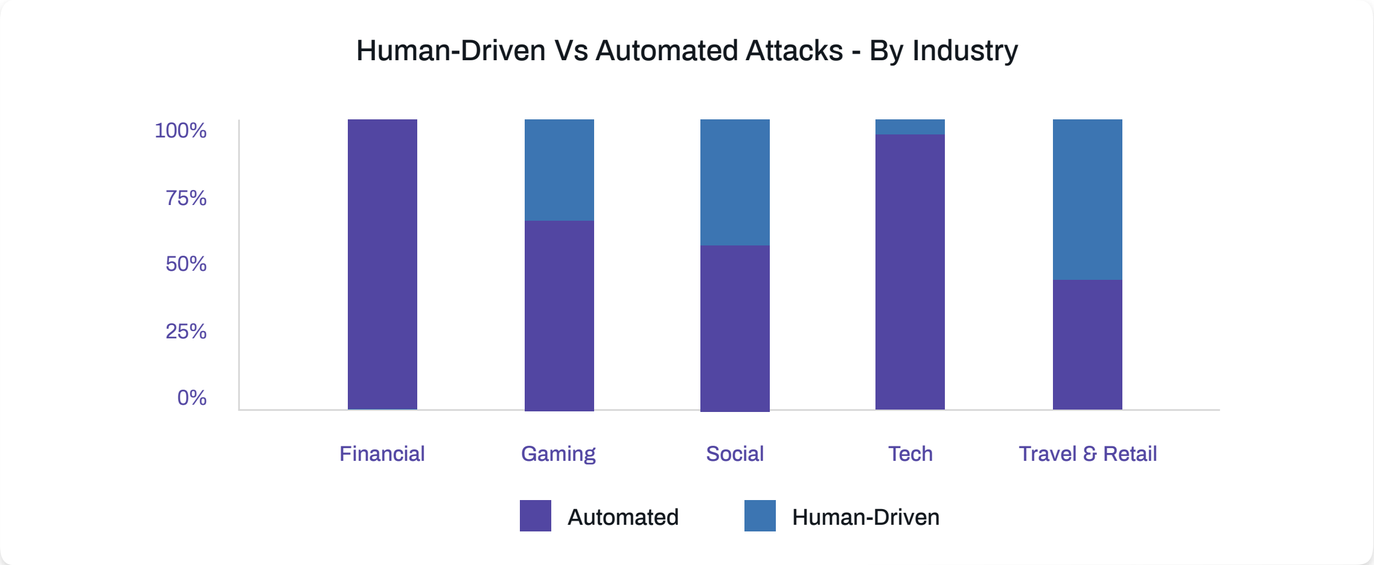
54% of retail & travel attacks from sweatshops. The nature of attacks on this sector have changed dramatically.

Increase in automated attacks on tech platforms. Fraudsters ramp up attacks quickly alongside changing traffic patterns.

Finance attacks dominated by automation. Large-scale credential stuffing attacks target logins.

24% increase in automated gaming attacks. Fraudsters using automated tools to increase attacks in line with the major spike in gaming activity.

1/3 of social attacks are human-driven. Shifting attack patterns following very elevated levels of sweatshop attacks last quarter.



Level Up: Fraudsters Flock to Online Gaming

27% increase in attack rate

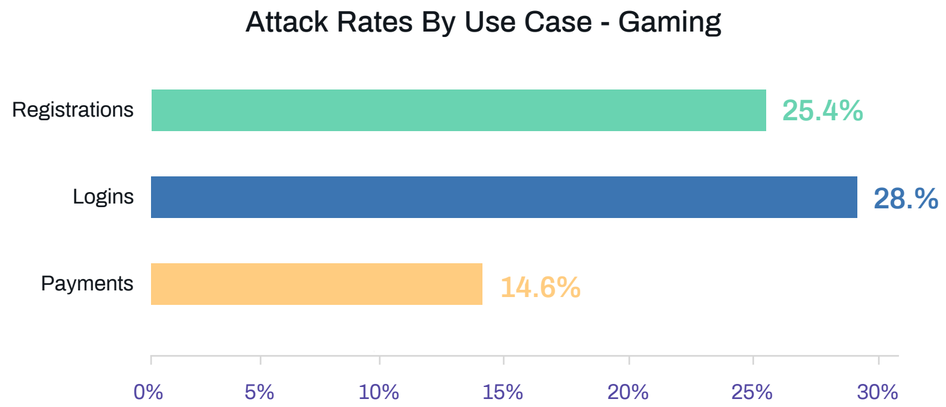
40% attack rate from desktop traffic

Logins
most-attacked use case

As legitimate consumers increase their usage of online gaming, this puts the industry directly in the line of fire of fraudsters, who ramped up attacks at the end of Q1 looking to blend in with legitimate traffic.

27% of all transactions on online gaming platforms are fraud attempts, making it a top attacked industry. Logins are the most attacked touchpoint, but attacks on registrations are also high.

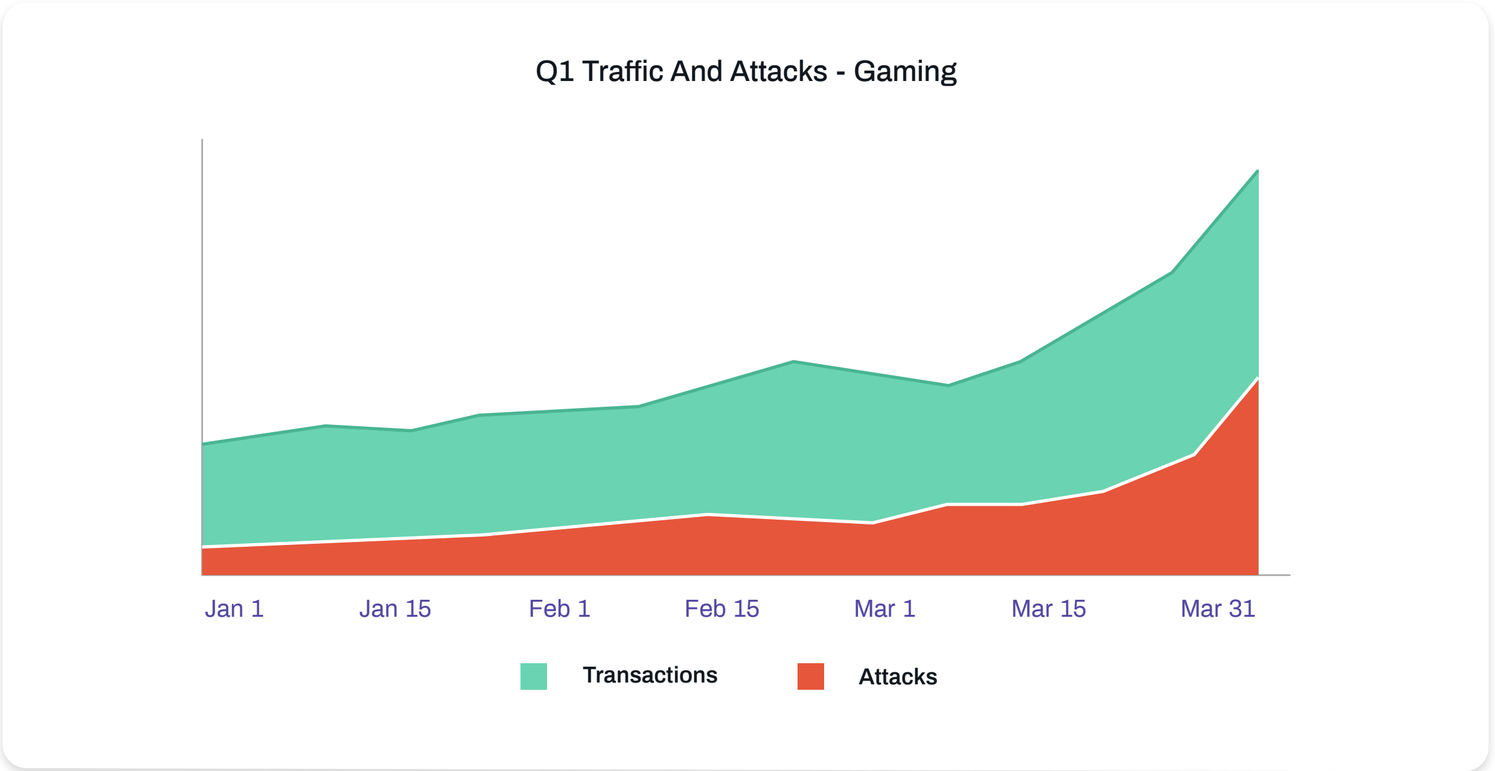
Fraudsters are primarily attacking from desktops, rather than mobiles and gaming consoles, using tried-and-tested techniques learned over time and shared among the fraud community.



Gaming During COVID-19: Every Day is a Holiday

The gaming sector is seeing the direct effect of the COVID-19 crisis. With both adults and children confined to the house, traffic is elevated and the usual weekend spikes have flattened out. There are now elevated traffic levels across the week.

Dramatic changes to consumer behavior over a short period of time can throw off existing fraud detection and behavioral analytic systems. Arkose Labs' gaming customers are benefiting greatly from their ability to validate risk assessments with results from enforcement challenges, at a time that good consumer behavior is abnormal and attacks are heightened.

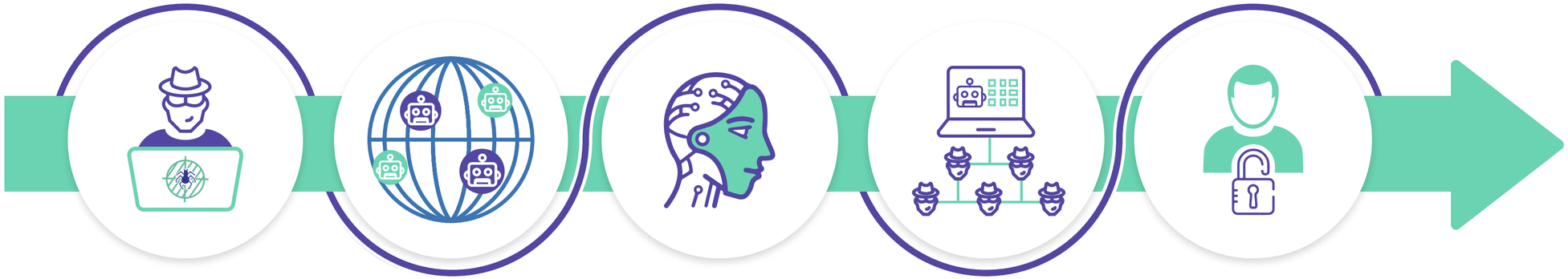


Case Study: Hybrid Attacks Target Online Gaming Platform

An online gaming company on the Arkose Labs network was being targeted with hybrid attacks displaying an advanced level of orchestration and sophistication. Fraudsters deployed a mix of automated tools and human resources, tapping into an on-demand network of sweatshop workers to increase their reach.

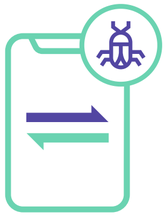
The primary attacker coded their bot to fill in the form automatically and then detect when it was presented with a challenge. The challenge was then farmed out to sweatshops for solving, using an application which connects to workers. Once the challenge was solved, the session was verified and the fraudster was able to register a new account.

Arkose Labs identified that the attack was coordinated by a single fraud ring by cross-matching the characteristics of the user initially filling out the sign-up form and the user completing the challenge. Everytime a new fraud ring or sweatshop is identified by Arkose Labs, all companies on the network are protected against downstream abuse.



Technology Platforms Face an Array of Fraud and Abuse Tactics

19.5% increase in attack rate

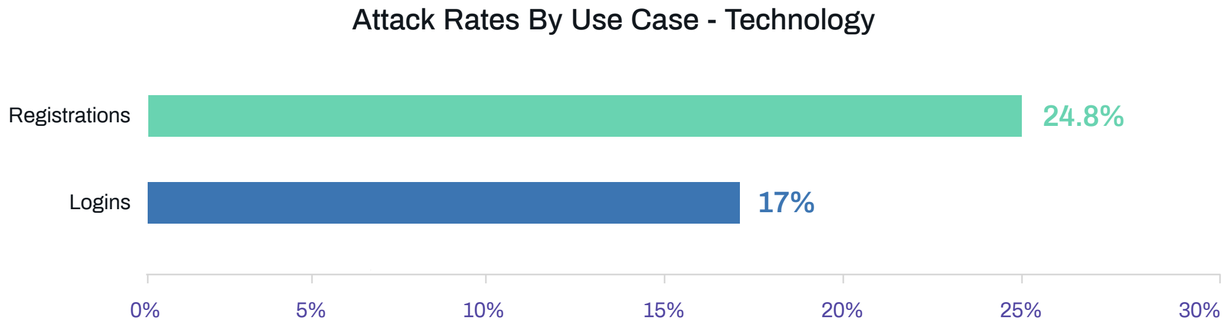


48% of mobile transactions are fraudulent

25% of registrations are attacks

As individuals move online for all facets of both their personal and corporate lives as face-to-face interactions shut down, technology platforms are another industry seeing elevated activity levels - from both legitimate users and fraudsters.

With many individuals setting up new accounts in order to connect, collaborate and communicate with their colleagues, friends and family, fraudsters looking to blend in with this traffic ramped up their attacks by 25% on new account registrations. Ever the opportunists, fraudsters shift tactics rapidly and fraud prevention teams at technology companies must stay on high alert for heightened levels of attack.



Case Study: Cloud Communications Platform

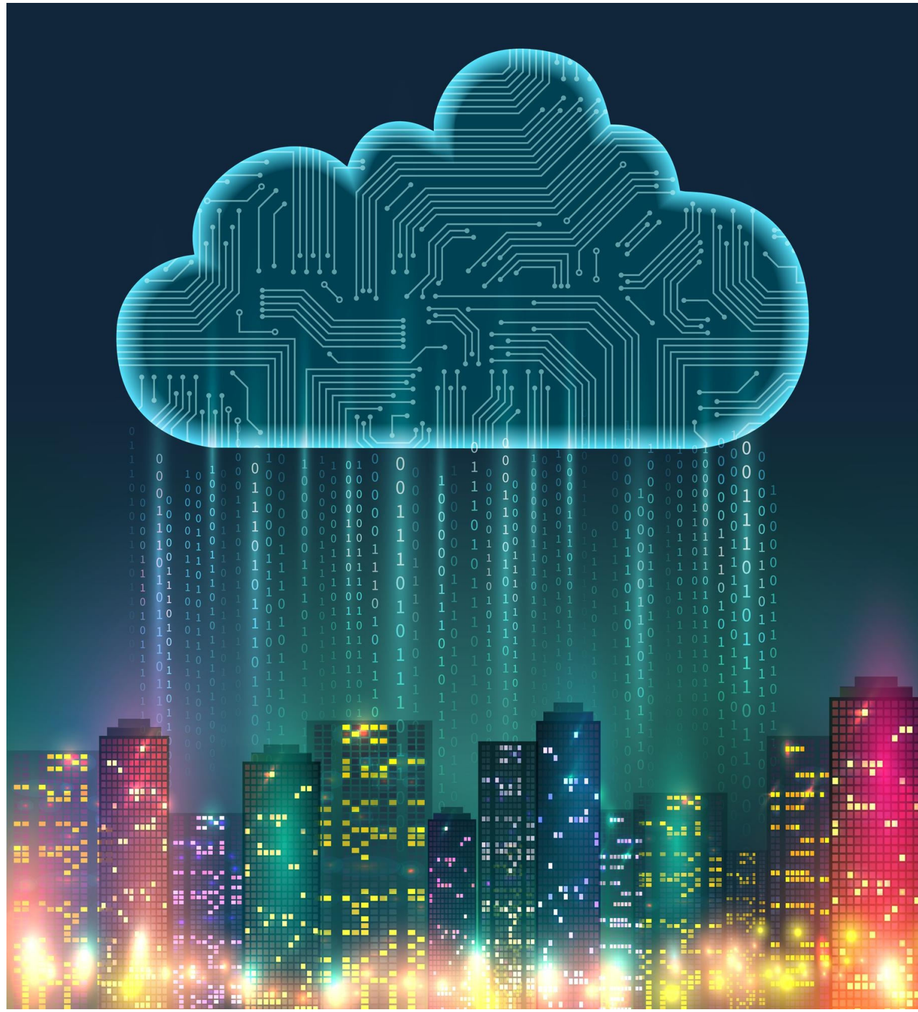
A company which enables software developers to use its web service APIs to programmatically perform a variety of communications functions, was offering a new user promotion in the form of phone credits. However, fraudsters were abusing this by setting up new accounts to call premium numbers and commit downstream fraud.

Solution

The company deployed the Arkose Labs platform, which enabled them to differentiate between good users and suspicious traffic. New users were shown enforcement challenges prior to their first email; for good users this meant minimal friction that did not affect the customer experience. However, adaptive step-up challenges sapped fraudsters' efficiency.

Results

Fraudulent new account originations were eliminated, which greatly reduced the the abuse associated with the mass dissemination of malicious emails.



Changing Attack Patterns on Social Media Platforms

24% increase in attack rate

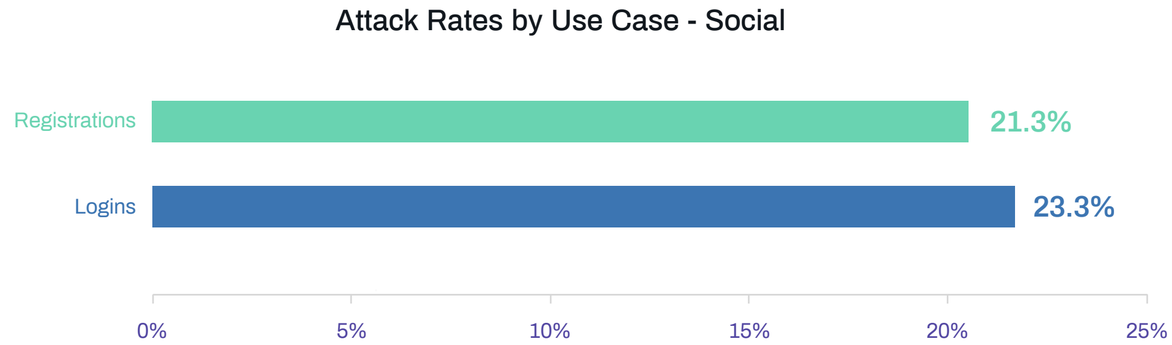
39% drop in attack rate since last quarter

31% drop in human driven attack

One-fifth of traffic on social media companies is an attack, however, there has been an overall decrease in attack rates compared to last quarter.

Account takeover attacks have reduced dramatically since last quarter, when we saw very elevated sweatshop-driven activity as fraudsters attempted to hijack accounts and defraud individuals downstream.

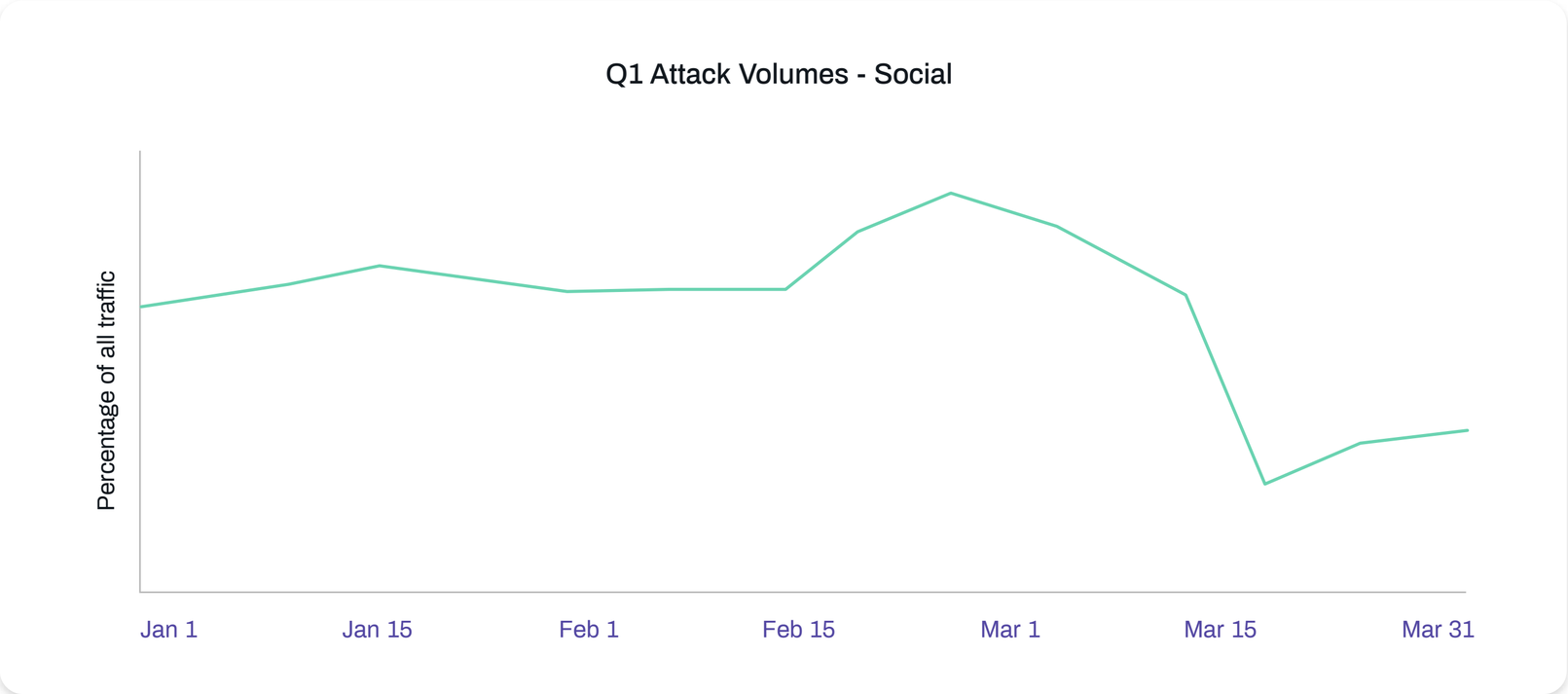
Although activity on social media remains high, as people connect and share news on evolving news stories, the dip in attack rates can be attributed to fraudsters refocusing their efforts on industries more on the frontline, such as ecommerce.



Love in the Time of Coronavirus

Online dating platforms provide an interesting example of adapting digital behavior during lockdowns. Data on the Arkose Labs network saw a seasonal rise in activity in February around Valentines Day, before a sharp drop-off as stay-at-home orders commenced.

However, online dating users were quick to adjust to the changing circumstances. Activity levels are recovering after an initial decrease in traffic. Individuals are increasingly embracing virtual first dates and online connections, rather than abandoning dating apps during lockdowns.



Case Study: Detecting Human-Driven Abuse on Online Dating

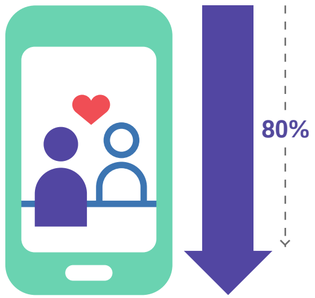
The online dating platform experienced an issue with “romance scams”, whereby fraudsters attempted to trick legitimate users out of money. These targeted human attacks are notoriously difficult for traditional fraud solutions to detect and the company was struggling to detect this activity until after the abuse occurred.

Solution

Arkose Labs deployed a mix of risk-based decisioning, behavioral analytics and targeted friction to identify and root out malicious users. The customer participated in an active data exchange, sharing characteristics of the fraud they saw downstream, enabling Arkose Labs to refine real-time detection at the account creation stage to provide early warning of malicious activity.

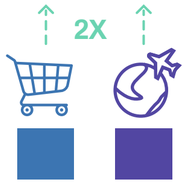
Results

There was an 80% reduction in fake account registrations. Downstream customer abuse and spam was prevented, safeguarding the interests of genuine users.



80% reduction in fake account registrations

Retail and Travel Changing Attack Trends



2x attack rate

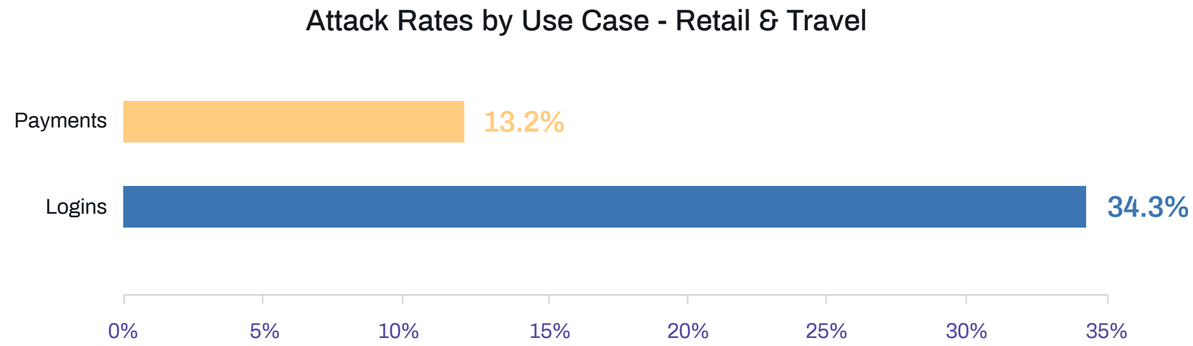
2.8x sweatshop attack rate

2.6x attacks on payments vs. logins

The retail and travel industries are both facing upheaval due to changes in consumer behavior amid the COVD-19 global crisis. While storefronts and travel companies are seeing business dry up, many ecommerce companies are facing an explosion in demand.

Fraudsters are focused on attacking payments, looking for routes to instant monetization. However, activity such as inventory hoarding is also of concern as it is offering unprecedented ROI due to shortages of essential items.

Due to the higher monetization potential, the volume of sweatshop-driven activity targeting this sector has skyrocketed.



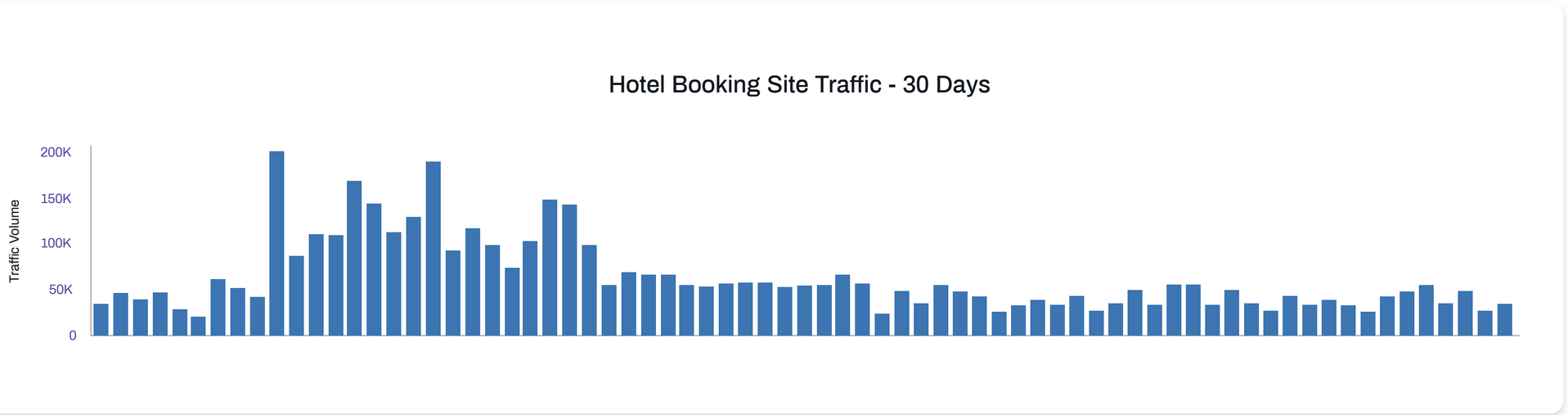
Retail vs. Travel: A Tale of Two Industries

Comparing the traffic and attack trends between retailers and travel companies highlights the complex repercussions of COVID-19.

Retail companies are seeing a far greater intensity of attacks, however, overall traffic volumes did drop slightly. Peaks in consumer shopping is inconsistent across retailers, with essentials and office supplies being highly in demand as lockdowns were introduced - whereas discretionary spend took a hit.

Travel traffic varied by region, with a 50% drop off in Europe, where COVID-19 had an earlier impact. The United States saw an overall increase in travel traffic, with a sharp decline at the end of the quarter.

Attacks accounted for a far greater proportion of retail traffic this quarter, and sweatshop-driven attacks leapt from one third to two thirds of attacks. On the other hand, travel saw an 85% drop in sweatshop-driven attacks with a 5% increase in overall attacks, driven by automation.



Fraud in the World of Finance and FinTech

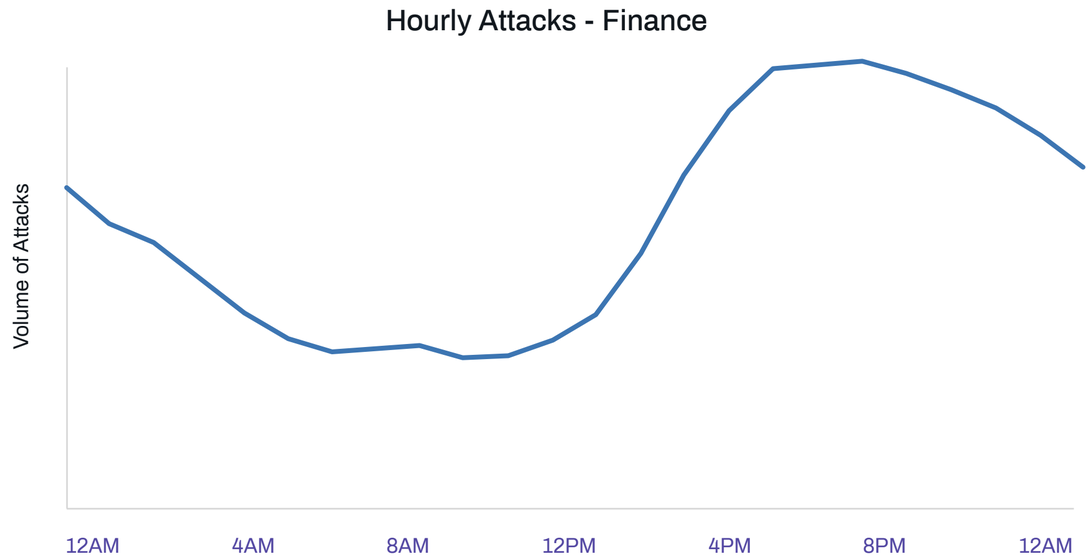
12% of all transactions are attacks

47% of all transactions are from mobile

Attack spike in the evenings

Finance and fintech companies are being targeted with a high level of automated credential stuffing attacks. Finance has the highest amount of mobile engagement, after social media, with nearly half of all transactions originating from mobile devices.

Interestingly, this quarter saw a noticeable shift in attack timings, with the bulk of attacks taking place in the evening, when previously it was more constant throughout. Fraudsters are trying to mimic genuine customer traffic, and stay under the radar of fraud prevention controls.



Conclusion

As the upheaval of the COVID-19 pandemic plays across different regions, the increased intensity of fraud and abuse attacks is predicted to continue, putting businesses and their fraud departments under strain.

Fraudsters are ramping up tried-and-tested ways to make money, looking to blend in with elevated digital traffic as society operates virtually, due to social distancing mandates.

Taking advantage of rapidly changing consumer behavior during lockdowns, cybercriminals are also exploring new attack vectors and executing large-scale spam and abuse. The longer that uncertainty and economic distress continues, the more people may become susceptible to scams that play on fear and emotion.

Arkose Labs is monitoring transaction and attack patterns closely during this crisis, and stamping out evolving fraud attacks for its customers as they emerge. It is more important that ever to stop fraud and abuse early in the customer lifecycle through proactive measures, keeping businesses, consumers and the economy safe during these tumultuous times.

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.
- Finance 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.

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.

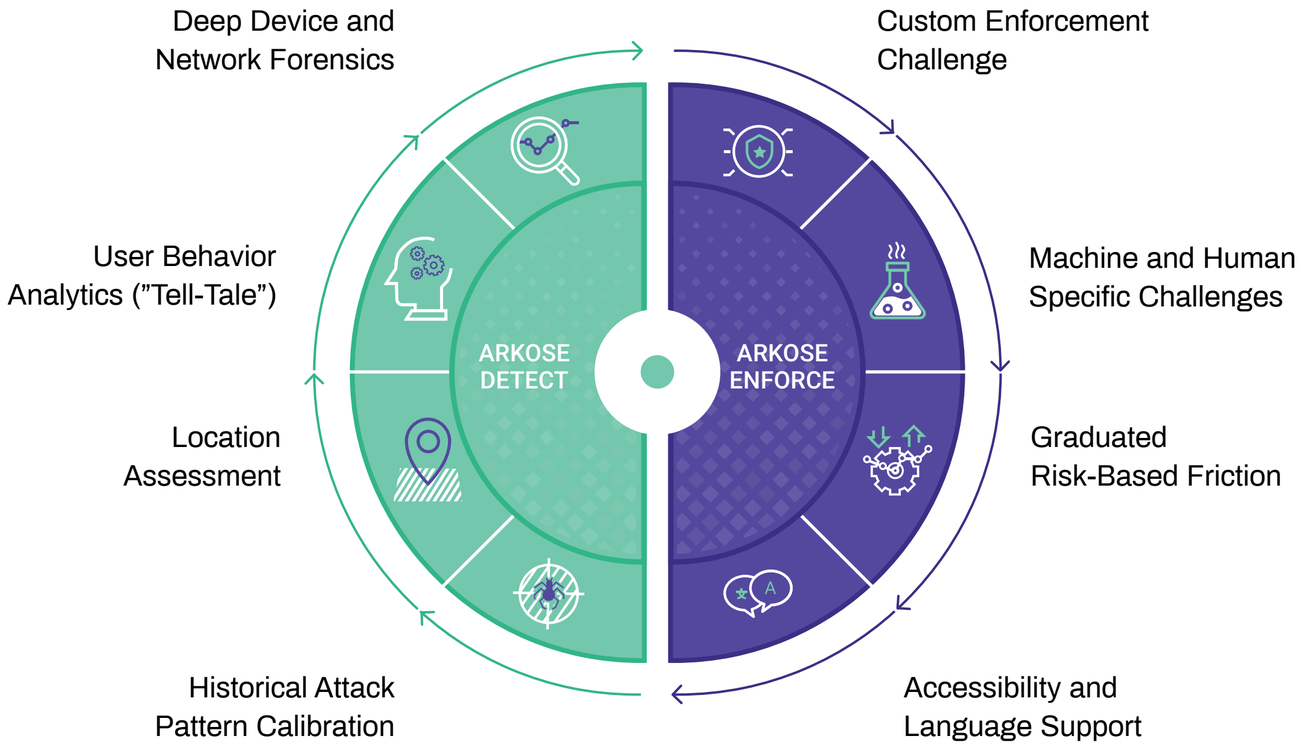
Fraud Types (cont.)

- 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.

Attack Types

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

Arkose Labs' Fraud and Abuse Defense Platform



Arkose Detect is Trained by Arkose Enforce Results

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