Arkose Labs

Fraud & Abuse Report

Q3 2019

Foreword

Much can be said about the new digital economy and how it has fundamentally changed customer behavior, and thereby the payments and commerce landscape. From transforming the financial services industry to disrupting the travel and entertainment industries, e-commerce has come a long way in the past decade.

However, one unintended consequence of this digital growth has been the rapid increase in fraud and online abuse. It has never been easier to connect with people across the globe on social media, gaming platforms or on digital marketplaces - and it has never been easier to launch large-scale automated/organized attacks on businesses from across the globe.

Fraudsters continue to target businesses for personal and sometimes political gain. While new and improved tools have become available for businesses to combat fraud, the techniques used by fraudsters have evolved in parallel.

Cybercrime is the biggest threat to companies and a huge burden for digital natives across the globe. With trillions of dollars lost each year, cybercrime represents massive financial costs and is presumably more profitable than the global drug trade.

The key here is understanding the financial motives of the fraudsters who continue to attack businesses. While the digital economy has led to a globally connected ecosystem, the socio-economic gaps persist, making it profitable to invest time and money to attack businesses.

While the traditional approach has been to use technology to stop the attacks, it is clear that the only way to deal with this problem is to address the issue at the core - by removing the economic incentives for fraudsters, making attacks economically irrational, and pushing professional fraud operations beyond the window of economic viability.

Kevin Gosschalk
CEO & Founder, Arkose Labs

Report Overview

The Arkose Labs Q3 Fraud and Abuse report is based on actual user sessions (transactions) and attack patterns that were analyzed by the Arkose Labs Fraud and Abuse Prevention Platform from April 1, 2019 to Jun 30, 2019.

→ These sessions, spanning account registrations, logins and payments from financial services, e-commerce, travel, social media, gaming and entertainment were analyzed in real-time to provide insights into the evolving fraud and risk landscape.

→ Unsophisticated attacks don’t result in a user session and thus have not been included. The report focuses on attacks from sophisticated 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/sweatshop driven attacks. These attacks focus on defrauding the businesses and end users credentials through fraudulent account registrations, account takeovers or payments using stolen credentials.

→ Arkose Labs uses a bilateral approach that combines global telemetry with a patented enforcement challenge to generate large volumes of data on users, which is analyzed and acted on in real time. This provides unprecedented insights into attacker identification and classification, enabling the platform to deploy appropriate responses and countermeasures.

→ Suspect sessions are identified based on “tell-tales” classified as abusive/malicious by the Arkose Labs based on the historical attack patterns and network intelligence.

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

Report Highlights

Arkose Labs analyzed over
1.2 billion
transactions across multiple use cases and industries

11% of all sessions are attacks

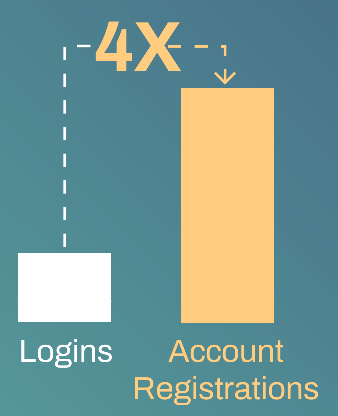
Logins represent
3 out of every 4
transactions

Over **1/2** of the login traffic on social media is illegitimate

Nearly **1/3** of all account registration attacks come from malicious humans (both one off and organized fraud sweatshops)

53% of account registration attacks for tech companies are human driven

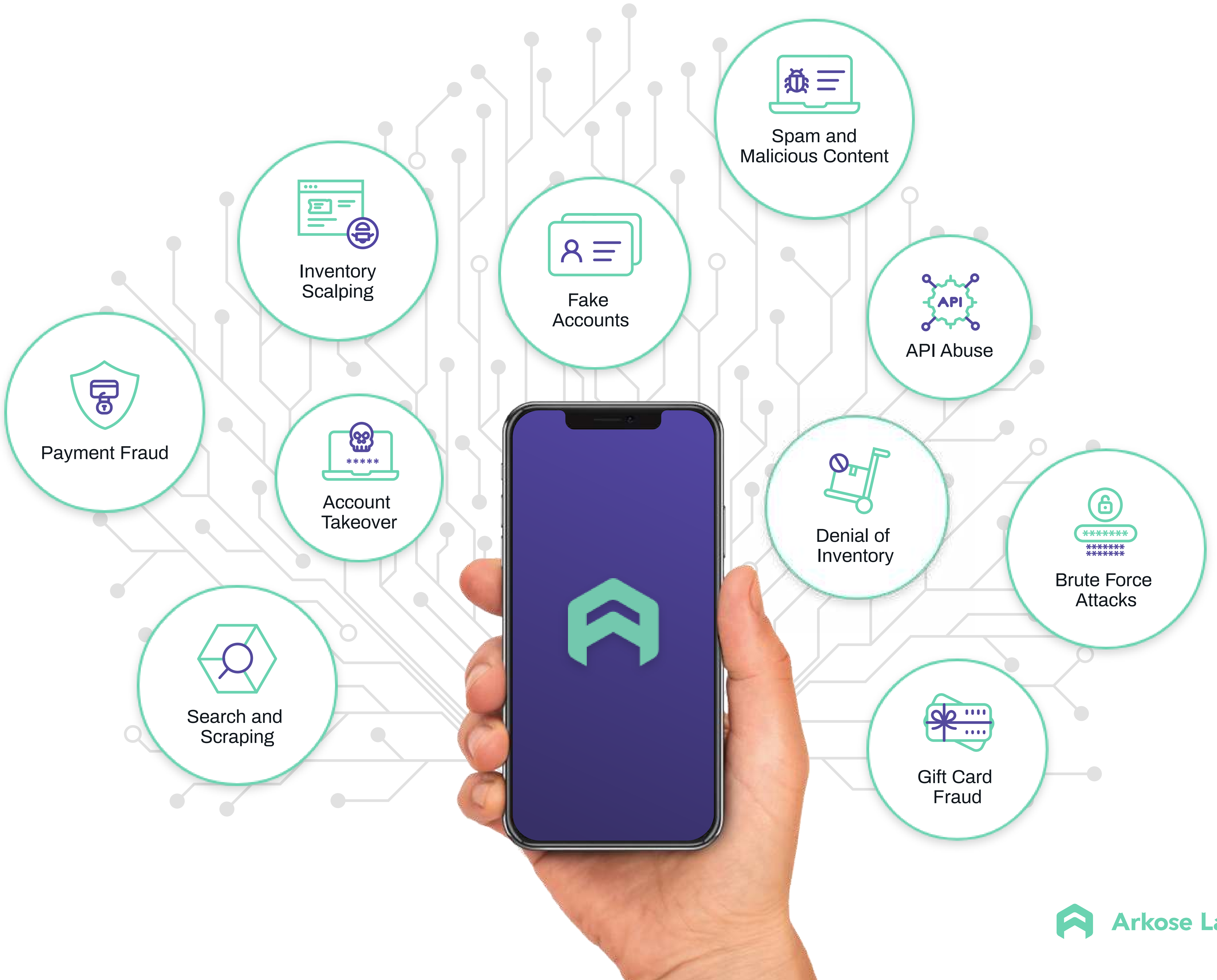
Payment transactions for travel see a high percentage of automated attacks that focus on **denial of inventory**

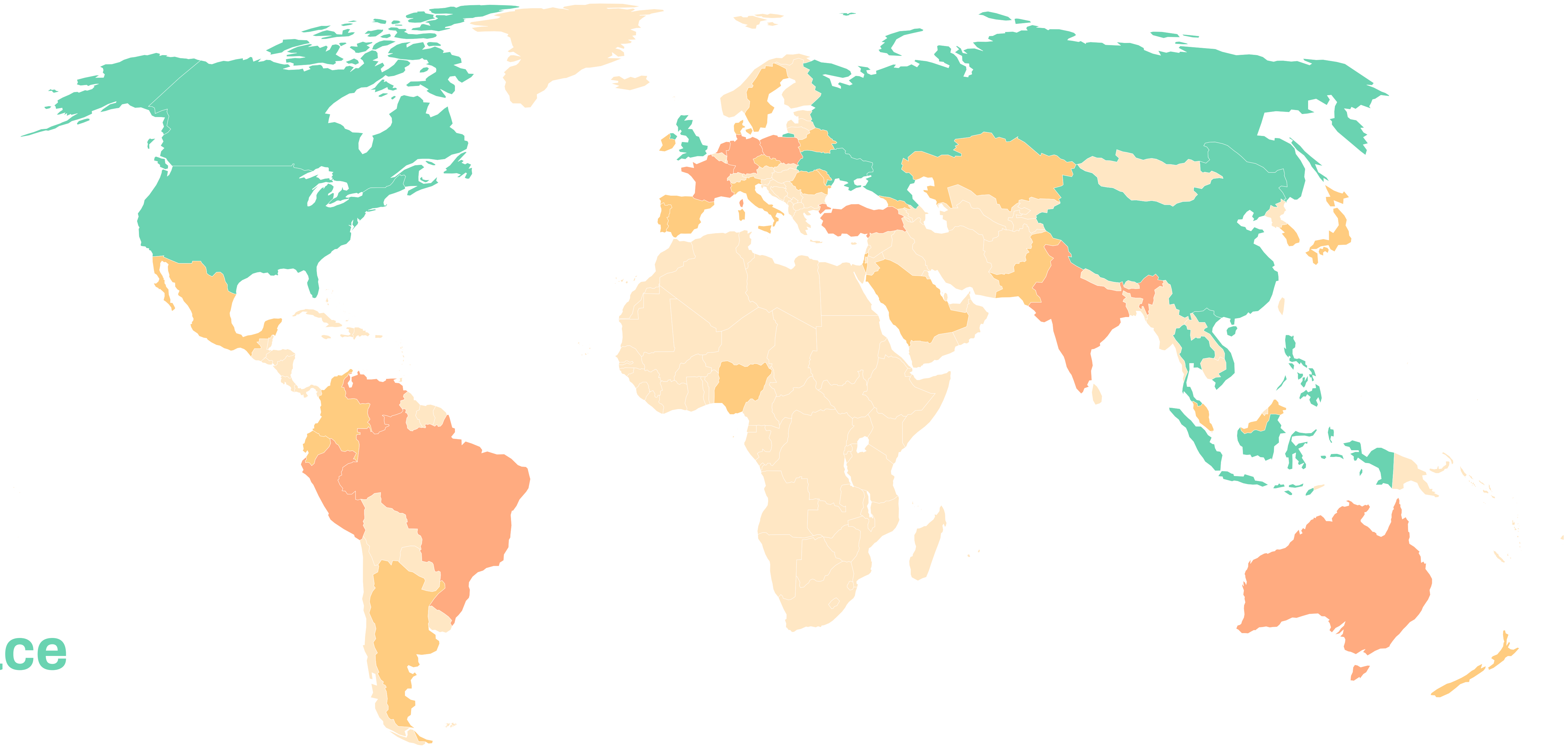


Account registrations for tech companies are **four times** more likely to be attacks than logins

Emergence of **single request attacks** that bypass traditional bot mitigation products by mimicking human traffic

Evolving Fraud and Risk Landscape





Global Attack Patterns - The Race to Monetization

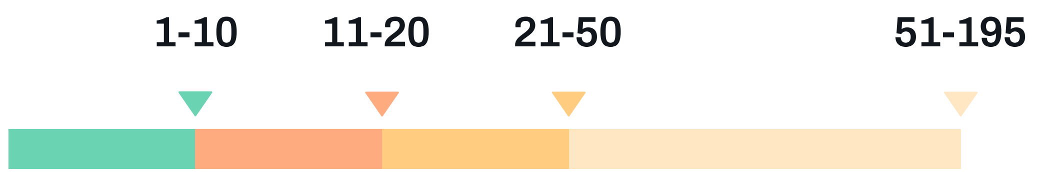
Global digital businesses, founded on technology, actively look to engage with customers across the world. At the same time, fraud and online abuse is on the rise, as cybercrime has become a big moneymaker for fraudsters worldwide.

Global availability of stolen and breached user data is shifting the base of cybercrime worldwide.

Developing economies are quickly becoming fraud hubs driven by easy access to sophisticated tools, availability of manual labor and good economic incentives associated with online fraud.

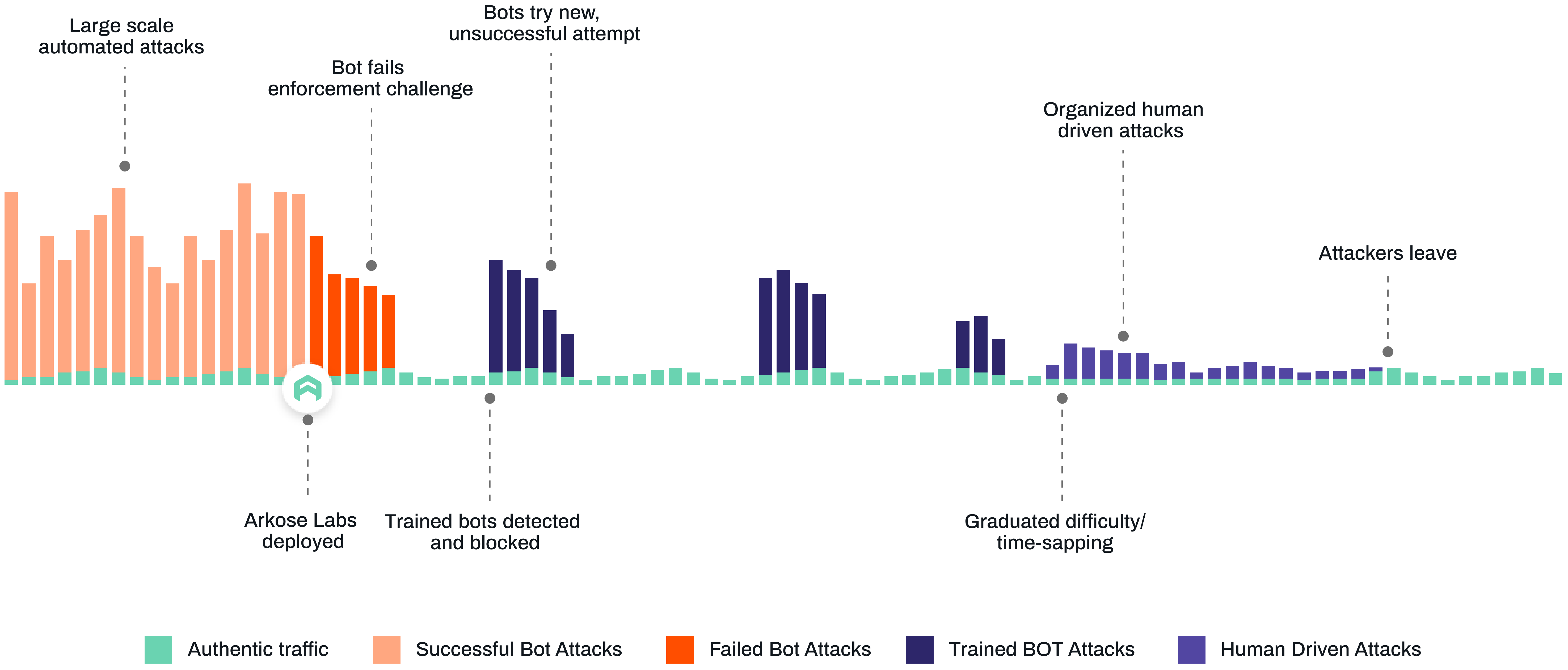
US, Russia, Philippines, UK and Indonesia have emerged as the top originators of attacks.

Top Attack Originators



Anatomy of Attacks - Evolution and Mitigation

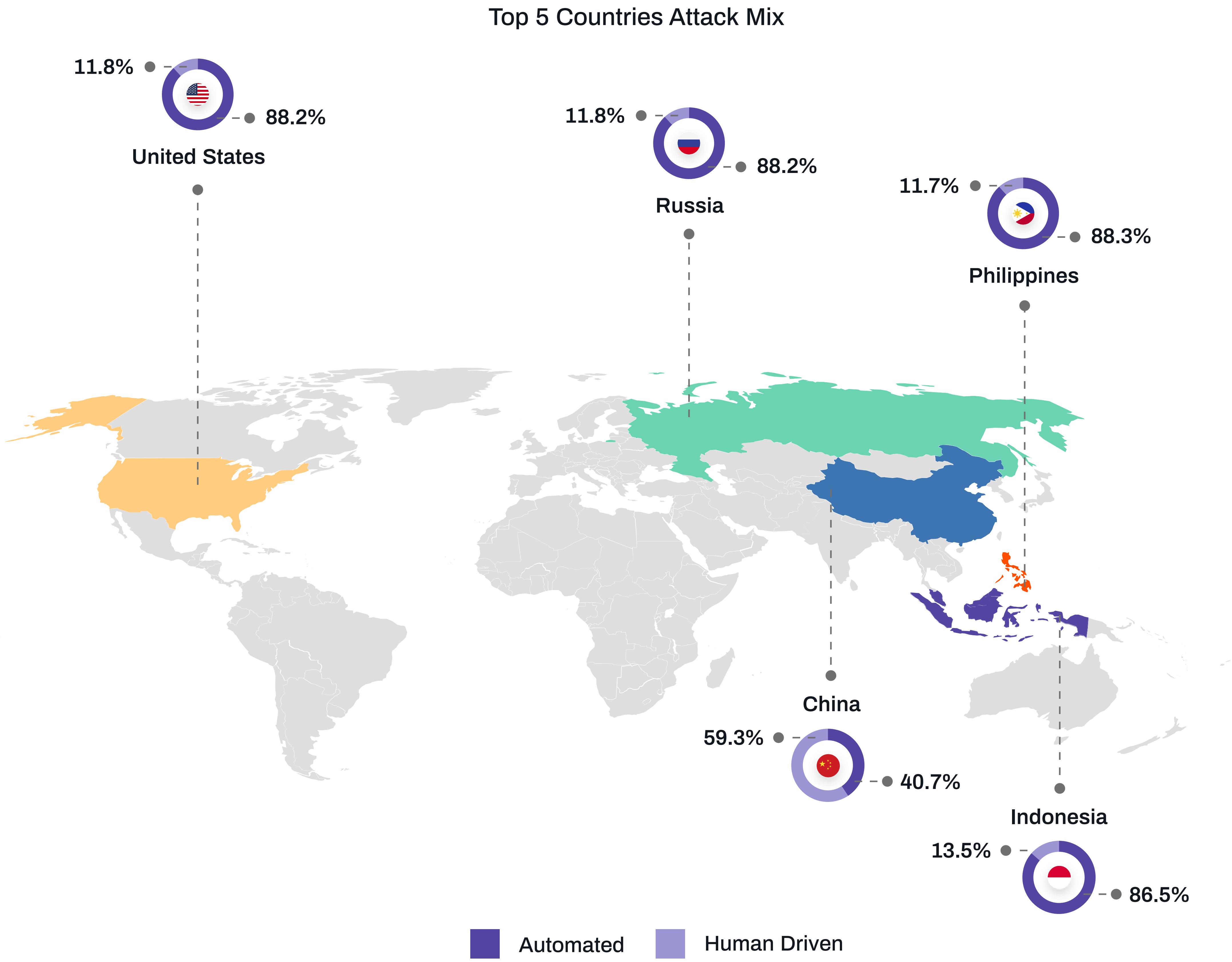
The connected fraud and abuse ecosystem means the attacks evolve as mitigations are deployed. Simple BOT attacks are followed by highly sophisticated BOT attacks that mimic human traffic. Once the BOTs are solved for, the human sweatshops/clickfarms are the next problem. They are quickly becoming the next wave of automated attacks where the fraudsters have access to large human workforce to launch organized attacks.



Top Attack Originators and Their Attack Mix

Automated attacks represent the bulk of the traffic, ranging from large-scale account validation attacks, to bots blocking seats on an airline to scripted attacks to scrape user data/inventory. However, sometimes fraudsters have to rely on a humans to carry out attacks. Although human driven attacks may cost more, the value they can extract from the attack makes the investment worthwhile. By exploiting the socio-economic gaps between developed and emerging economies, organized fraud rings have been able to wreak havoc on businesses.

The attack mix also varies by country. Philippines is the single biggest attack originator across both automated and malicious human traffic with US a distant second. Meanwhile, attacks from China are primarily human driven.

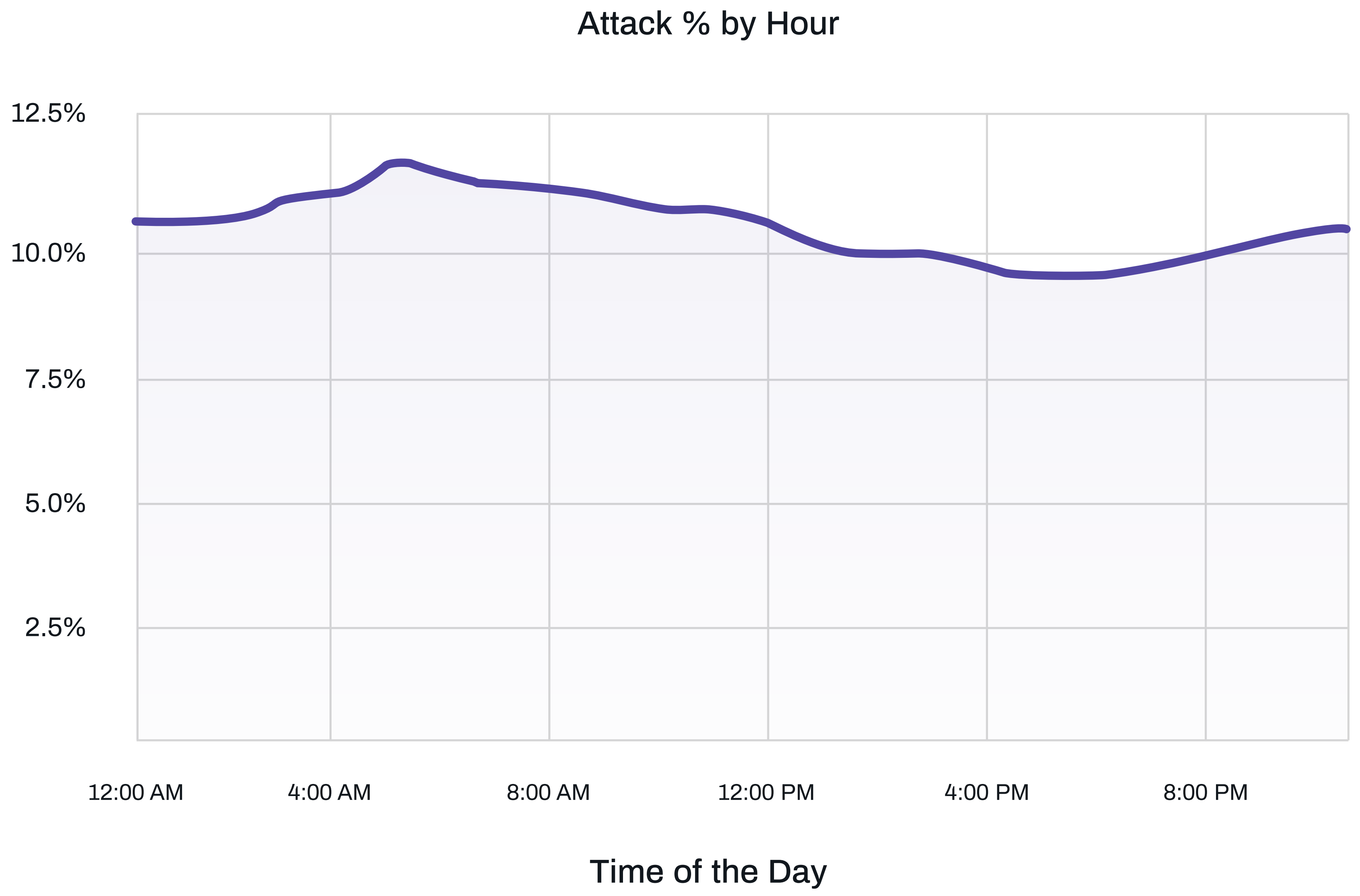


Attack Patterns Over Time

The global digital economy is always on, which means businesses are increasingly serving customers across multiple time zones and channels. This provides fraudsters with an opportunity to launch 24/7 attacks using tools that spoof location and mimic genuine traffic.

The timing of attacks provides an indication of the true location as fraudsters are increasingly operating like legitimate businesses, working in shifts and conforming to local business hours.

For use cases that require two-way interaction/thoughtful engagement, this pattern is especially visible. This further demonstrates that the "sweatshop" attackers are services operating across many industries.



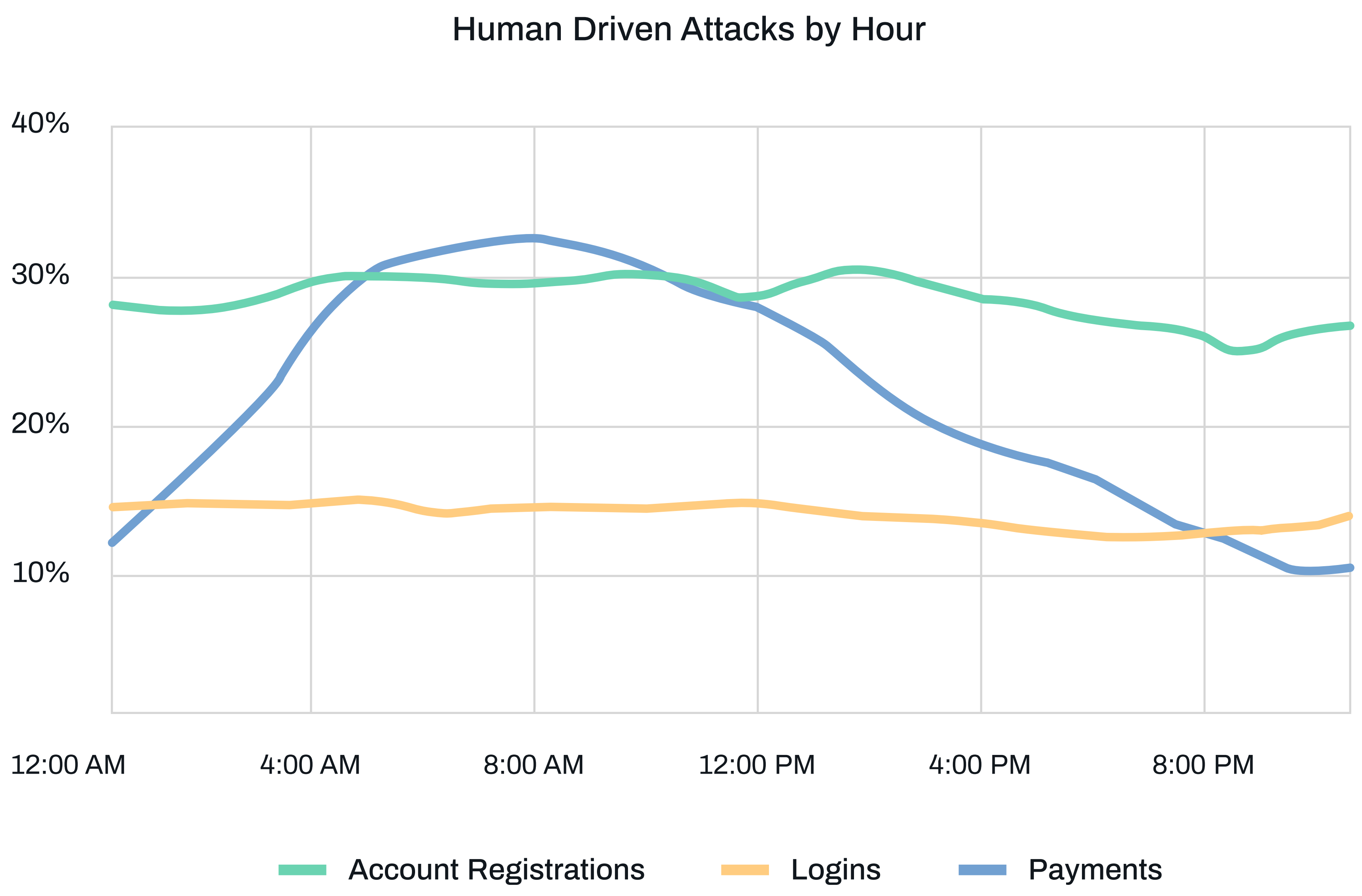
Human Driven vs. Automated Attack Mix - By Use Case

Unlike bot traffic, inauthentic human traffic is harder to detect as human behavior is unpredictable and highly nuanced. However, with closer analysis, interesting patterns emerge.

At a use case level, payment fraud and fake account creation are more likely to be carried out by humans, while account takeover attacks are commonly performed using automation. This is primarily because of the interactive nature of the use case when compared with a straightforward login event.

At an industry level, there is a variability when normalizing for the time zones. While technology companies target a global customer base and operate at all hours, retail and finance companies have 'business hours' that fraudsters try to mimic while hiding their true location.

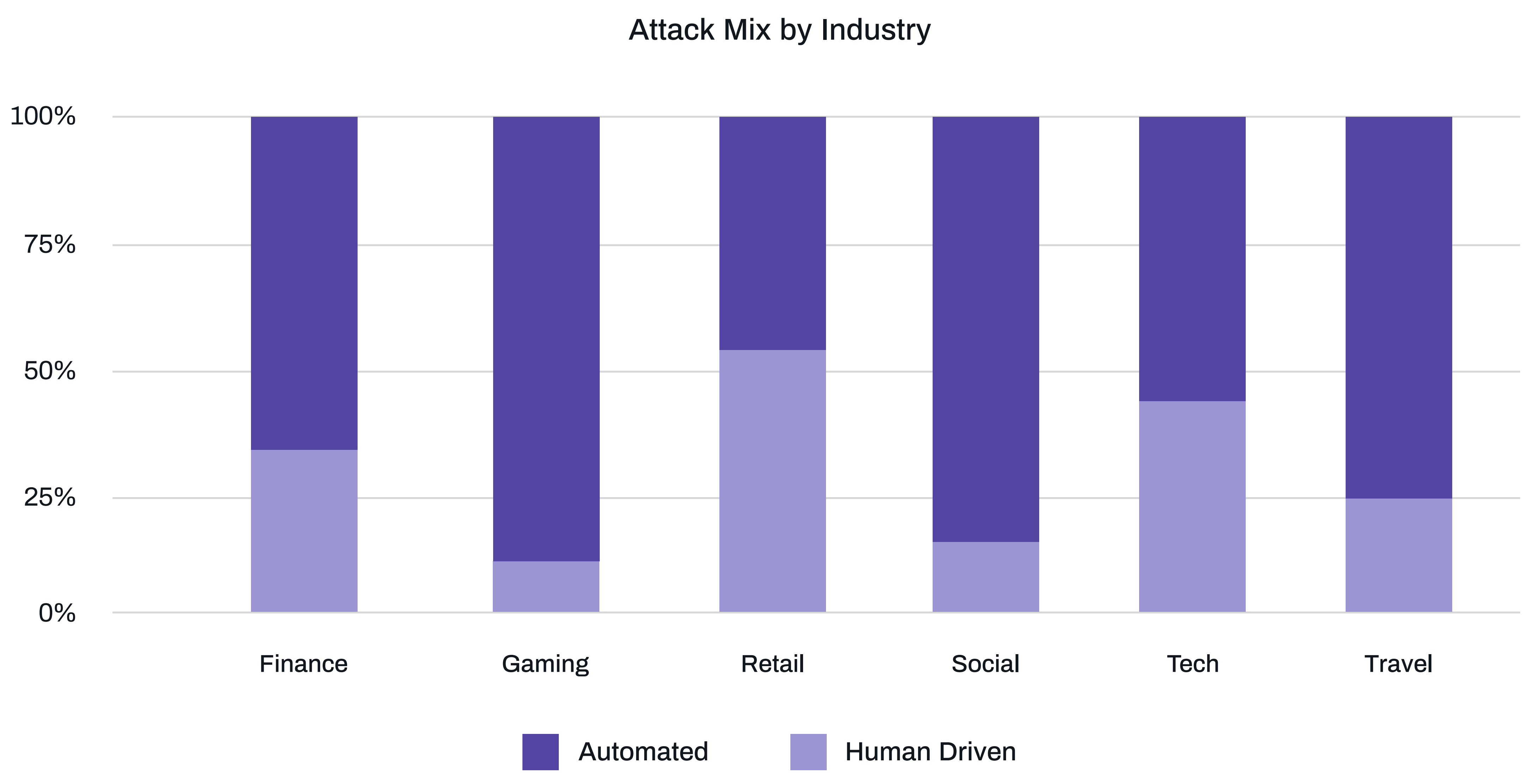
In industries targeted by a higher mix of human driven fraud, we see clear seasonality in traffic across the workday. This clearly indicates that the attackers operate in 'shifts' with time zones geared towards the attacked businesses.



Human Driven vs. Automated Attack Mix - By Industry

The mix of human driven attacks vary by industry and business model. Retail, finance and technology platforms witness the highest volumes of human attacks, since the most effective attacks often require human interaction.

While a lone fraudster can launch such attacks, there is an increasing number of sweatshops/click farms that employ a large group of low-paid workers hired specifically to make fraudulent transactions, write fake reviews, or create fake accounts using stolen/synthetic credentials.



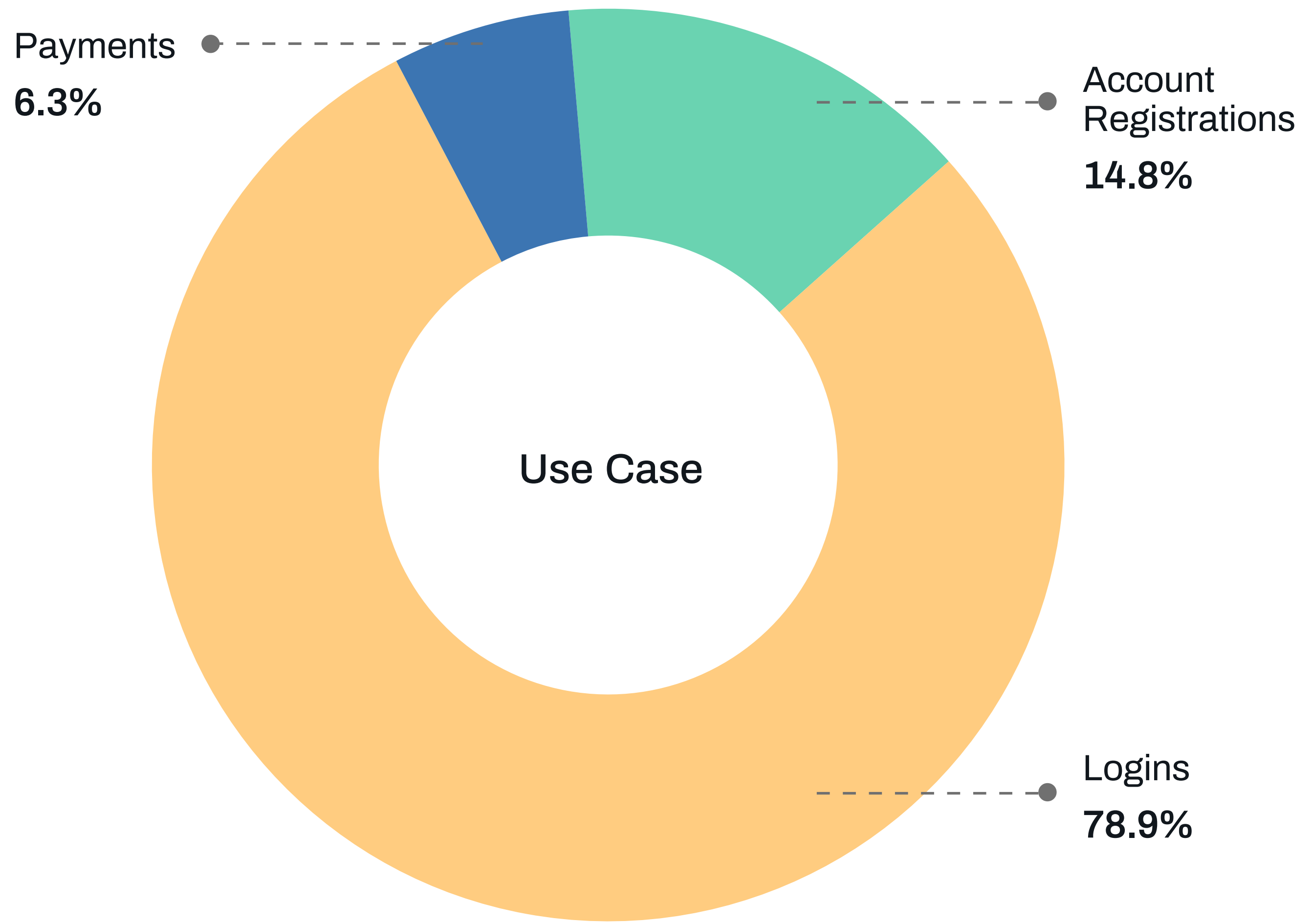
Fraud and Abuse by Use Case

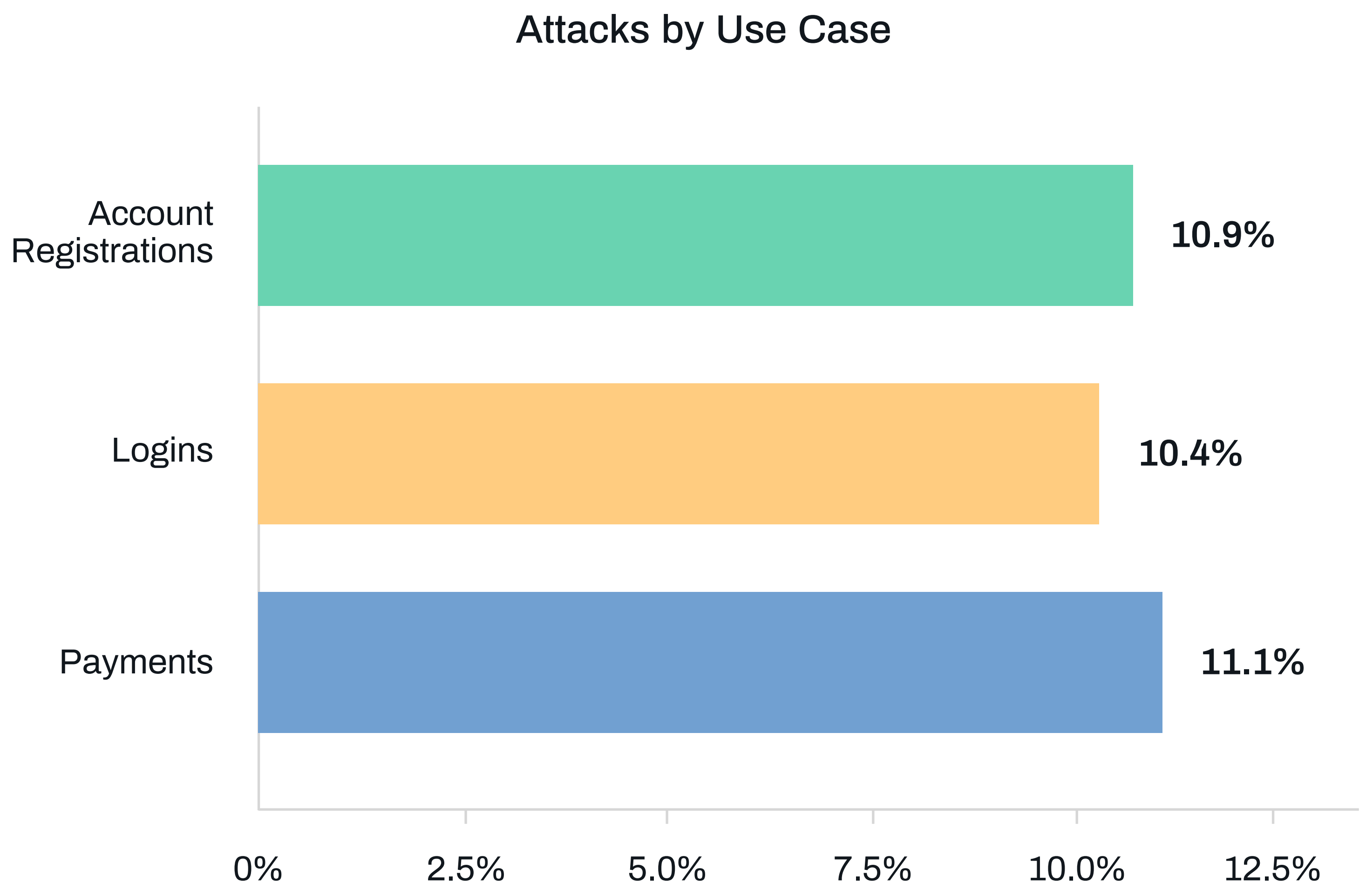
Businesses are leveraging the digital economy to target customers across the globe as they look to access services, make purchases, play online games or connect/interact with others. Arkose Labs' platform works with businesses across the entire customer journey that can be grouped under account creation, login, and payments.

As businesses have focused on close relationships with their customers, it is no surprise that logins constitute 3 out of every 4 digital sessions.

Digital is also the biggest channel for new customer acquisition. This is especially true for technology platforms, social media, travel and online gaming industries where the customer base is global.

At the network level, payment and account registration transactions are attacked only slightly more than logins. However, these attacks are 2.5X more likely to come from malicious humans.





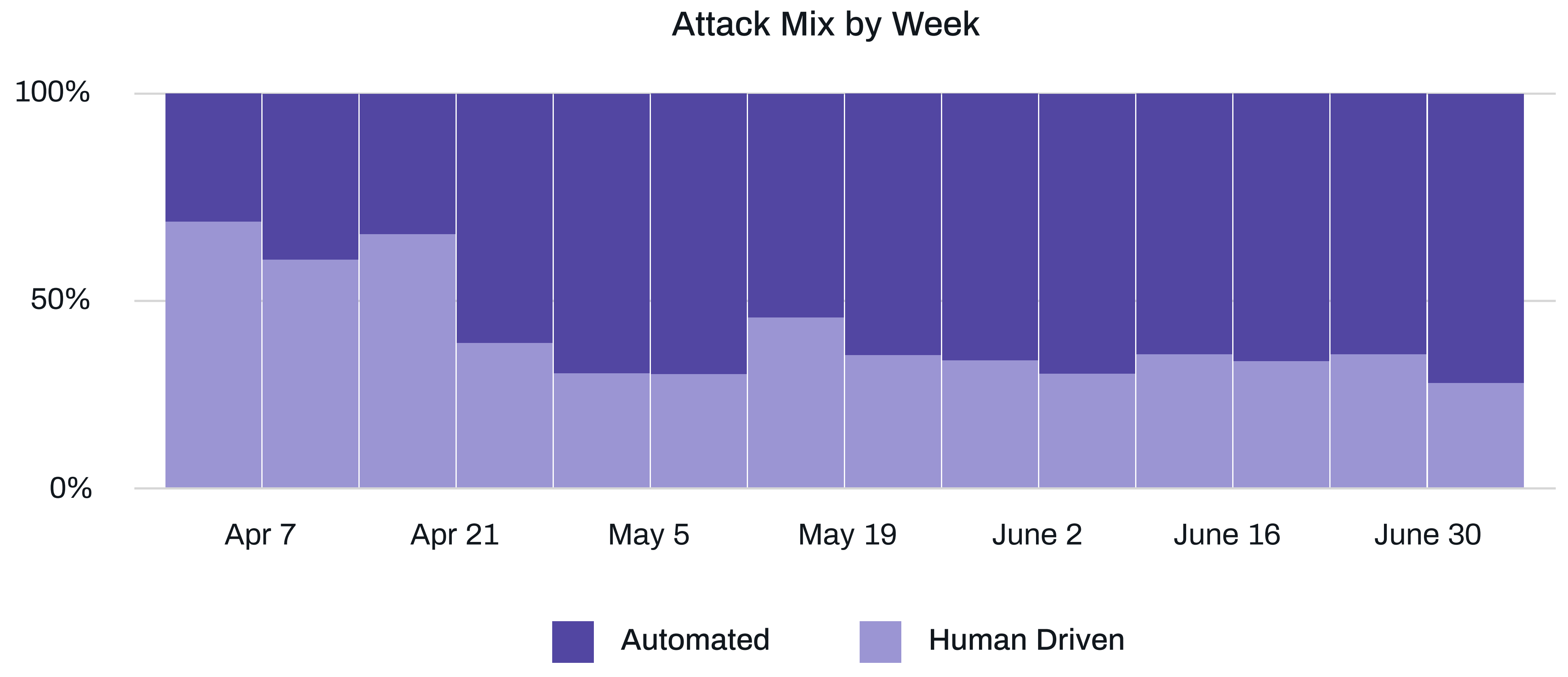
Finance and FinTech Transaction Analysis

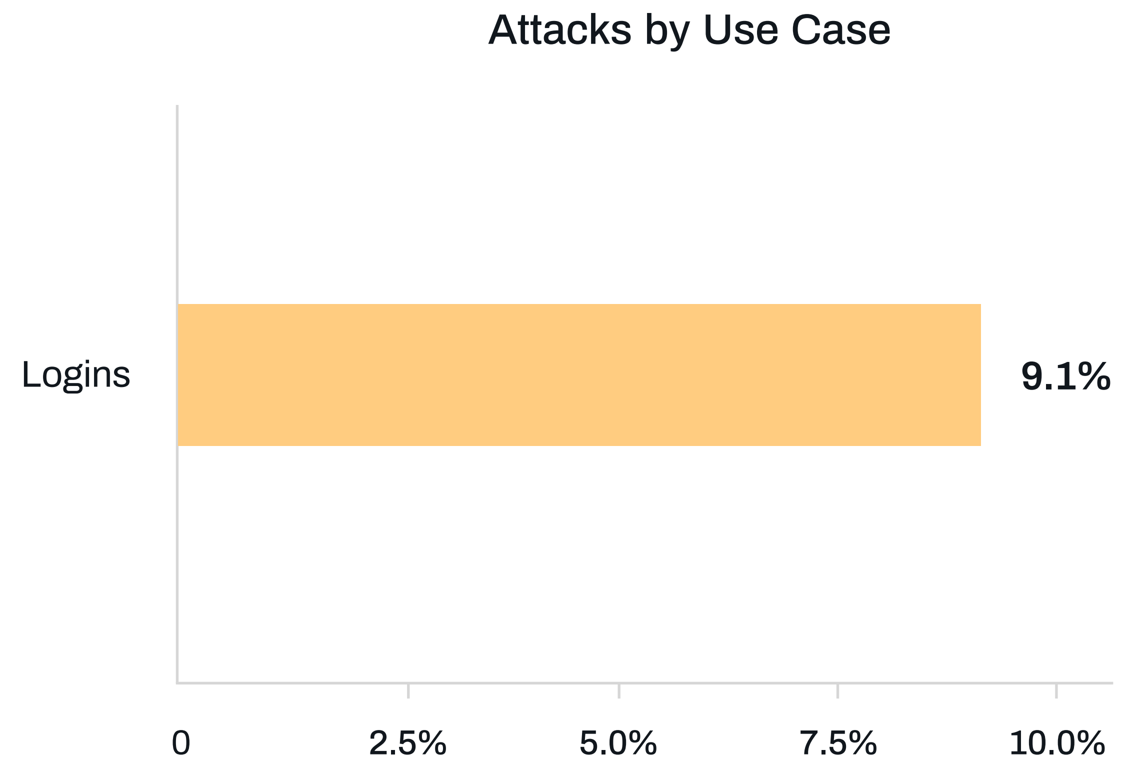
A major focus of Arkose Lab's deployment in Finance and FinTech is on protecting account logins and associated activities including balance check, account updates etc.

Arkose Labs has observed that 9% of the total login attempts are fraudulent with a third coming from human driven attacks. These attacks focus on taking over a legitimate user's account to transfer funds or sign up for fraudulent purchases.

The attack mix varies by the time of the day with fraudsters mimicking the daily user traffic patterns. At the same time, the financial services segment also witnesses seasonality in the attack patterns with attack volumes going up during high traffic periods like the tax season in the U.S.

Financial institutions are focused on getting users to access their accounts and will likely not decline the request. They will instead focus on stepping-up the transaction. The traditional methods of step-up, including KBA/SMS have become ineffective as fraudsters can easily bypass them with the help of stolen user data and tools.



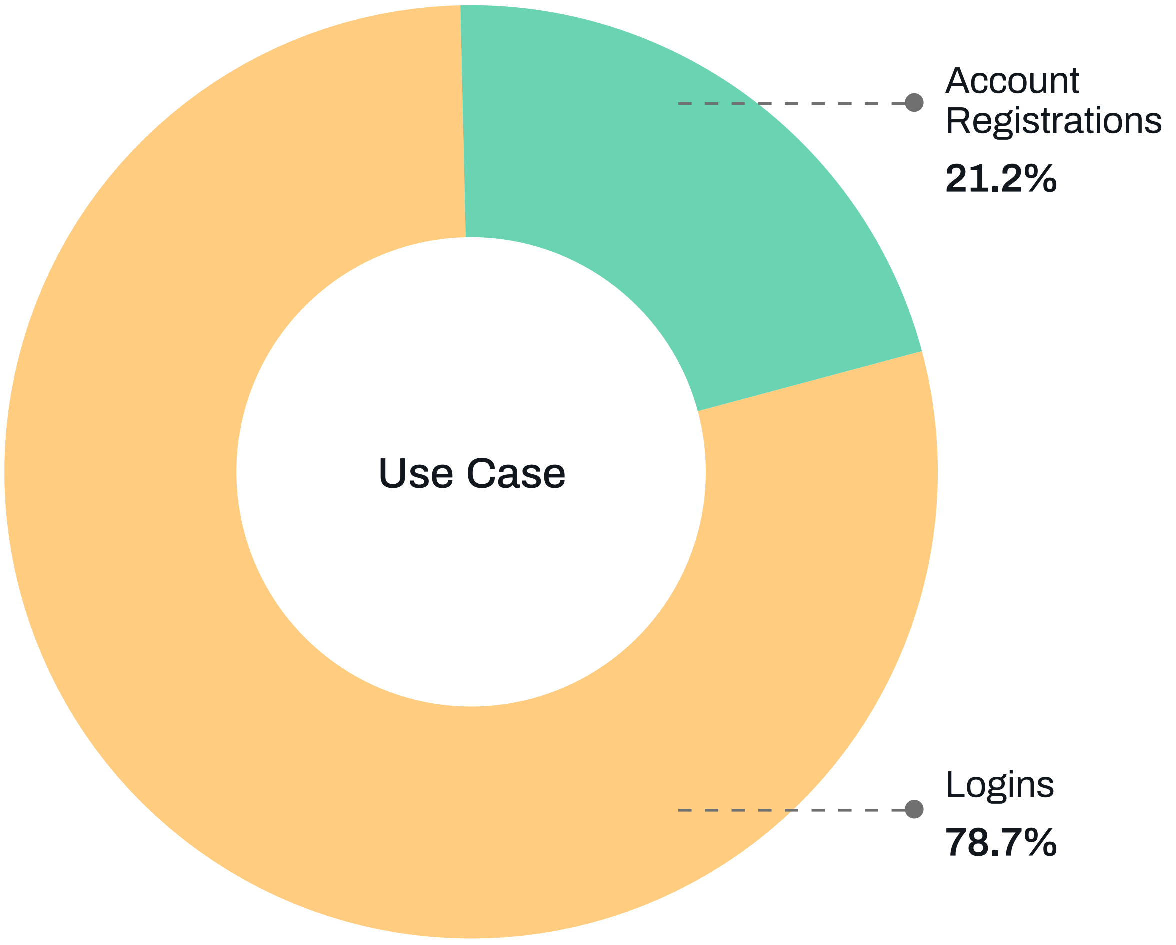


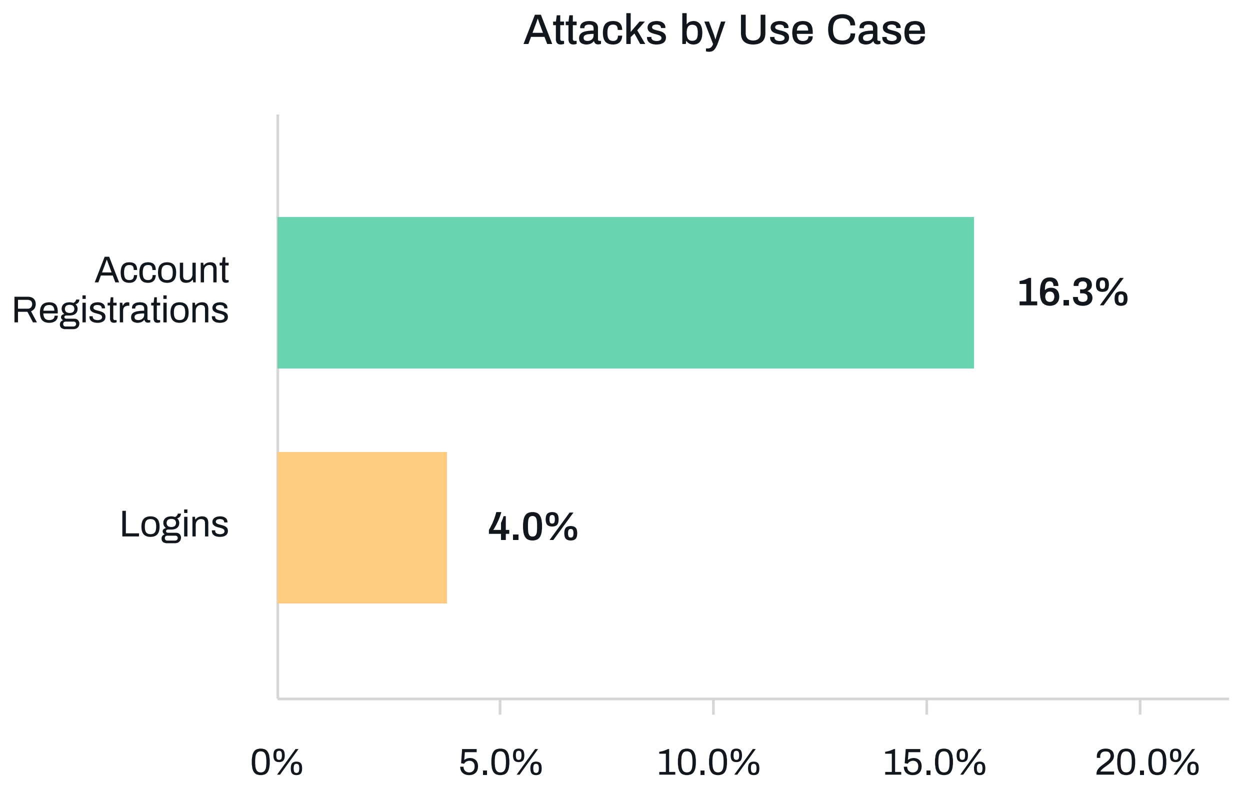
Tech Platforms Transaction Analysis

With businesses moving to the cloud, tech has emerged as a key segment offering access to distributed workforce. These range from communication platforms to storage to office tools.

Most tech companies offer a freemium model with quick/frictionless on-boarding for customers, making them an attractive target for fraudsters looking to either test stolen credentials or create fake account to access the services. This results in account registrations being attacked using both bots as well as organized sweatshops.

This segment is heavily targeted by human click-farms/sweatshops. Almost almost 43% of all attacks are human driven.



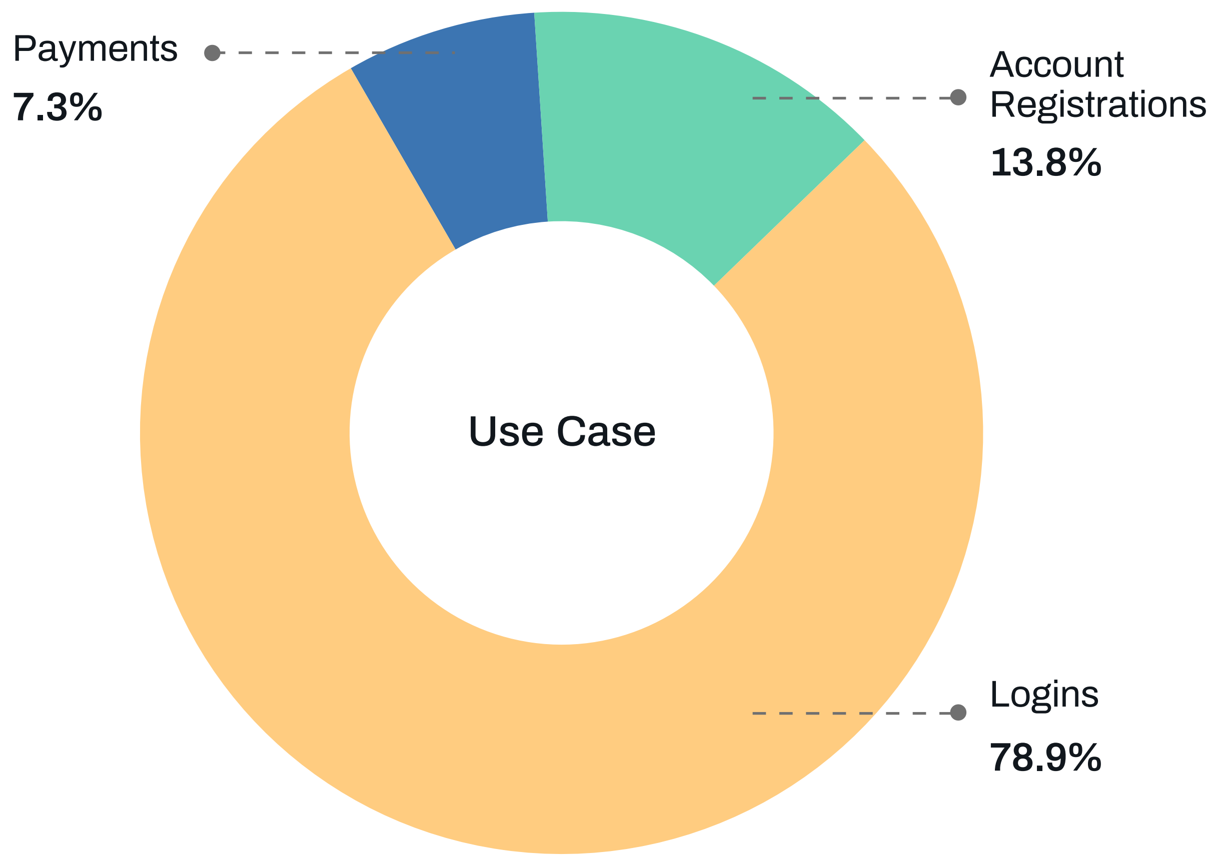


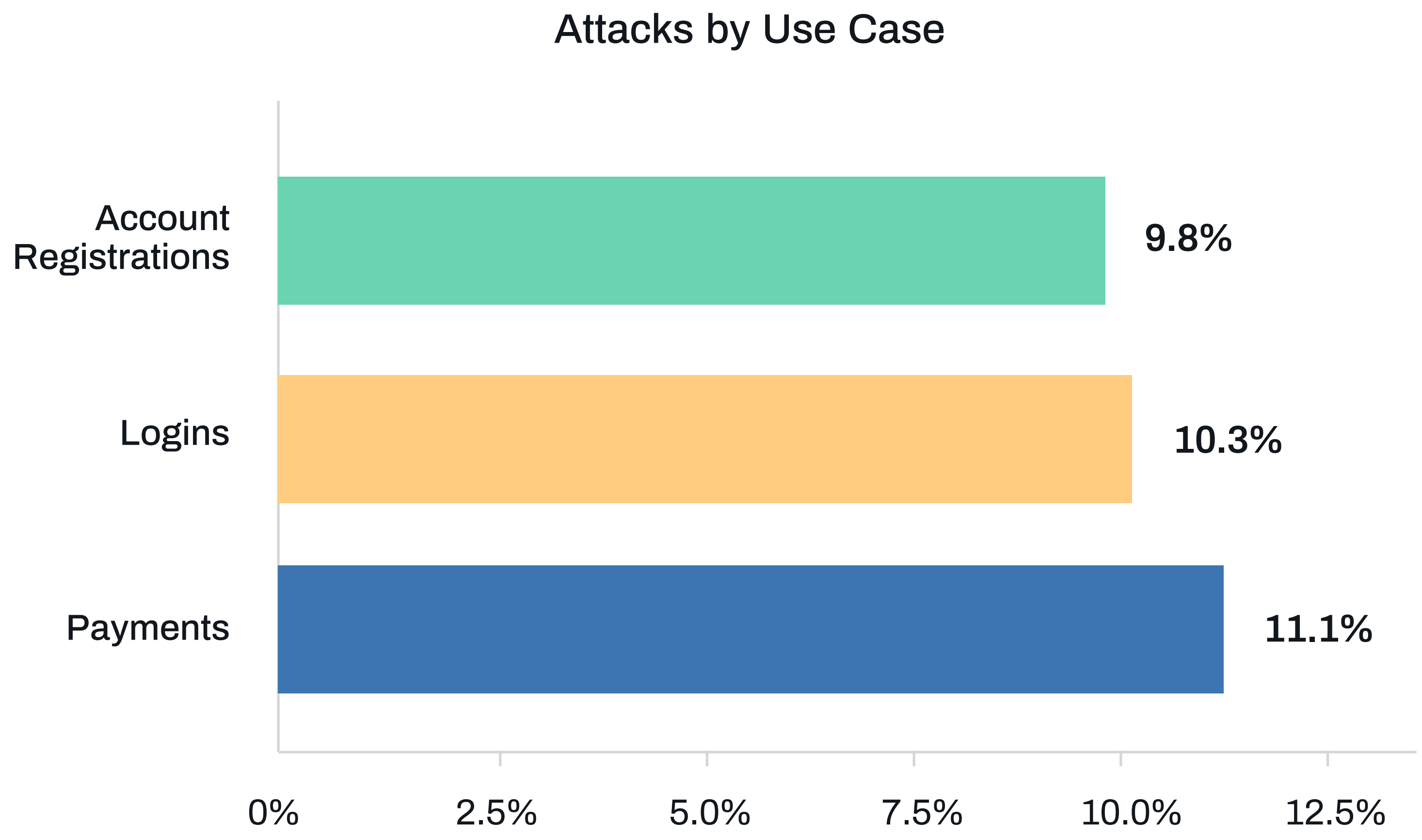
Gaming Transaction Analysis

The Gaming industry has one of the highest customer engagements, primarily driven by the popularity of online games that require high user involvement and time. With new games and in-game enhancements constantly getting launched, including the launch of new artifacts etc, account registrations and payments are also key use cases. Gaming platforms worldwide are focused on delivering exceptional customer experience while protecting the platform not only against attacks from fraudsters looking to monetize stolen credentials, but also from customers trying to 'game' the system.

By combining easily available user credentials with sophisticated tools, cybercriminals can orchestrate automated fraud at scale and extract monetary value in numerous ways. Criminals can resell accounts on third party markets or use these accounts to "gift" virtual goods to other players that drain money from the original account, which can then convert into chargebacks.

While attacks on gaming platforms are primarily driven by automation, certain use cases have high mix of manual attacks. These attacks are primarily driven by the need for two way interaction that requires human intervention.



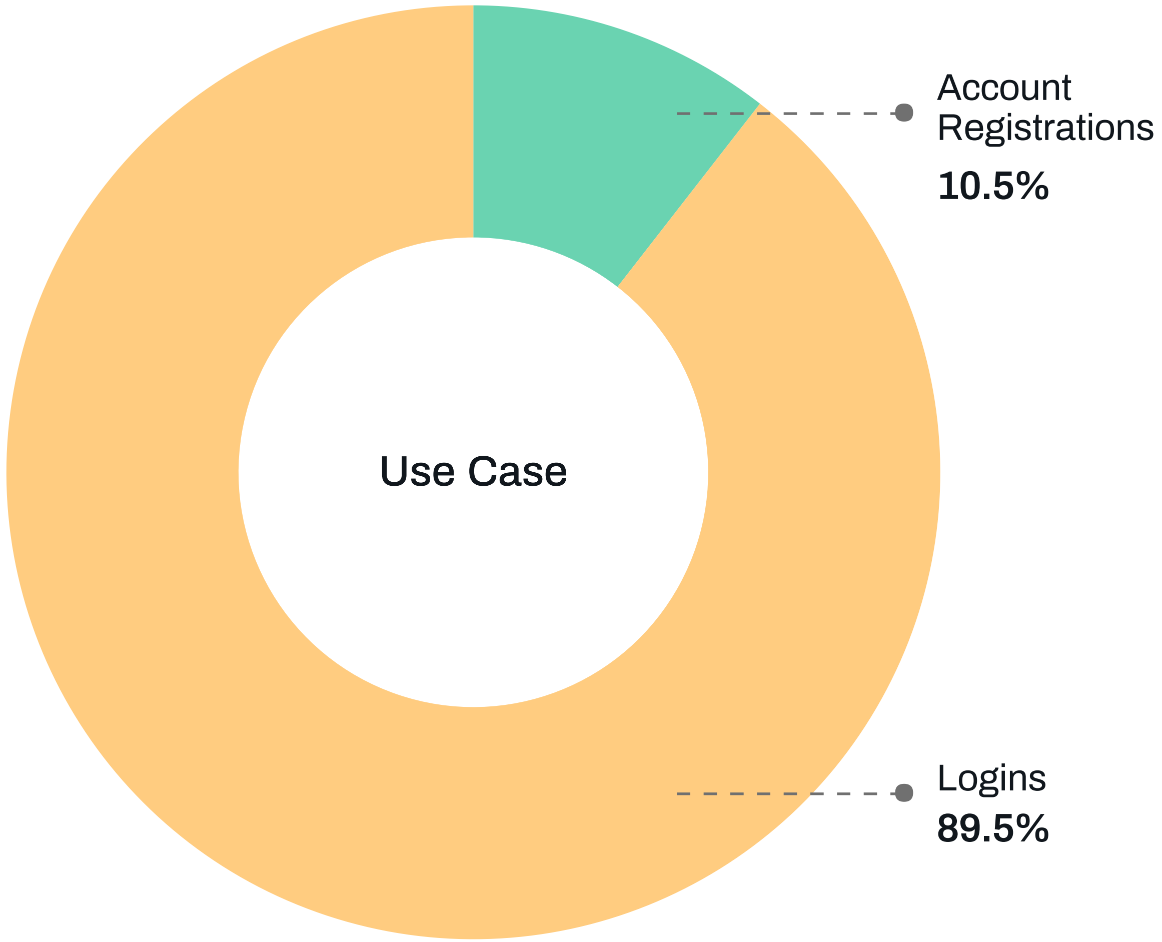


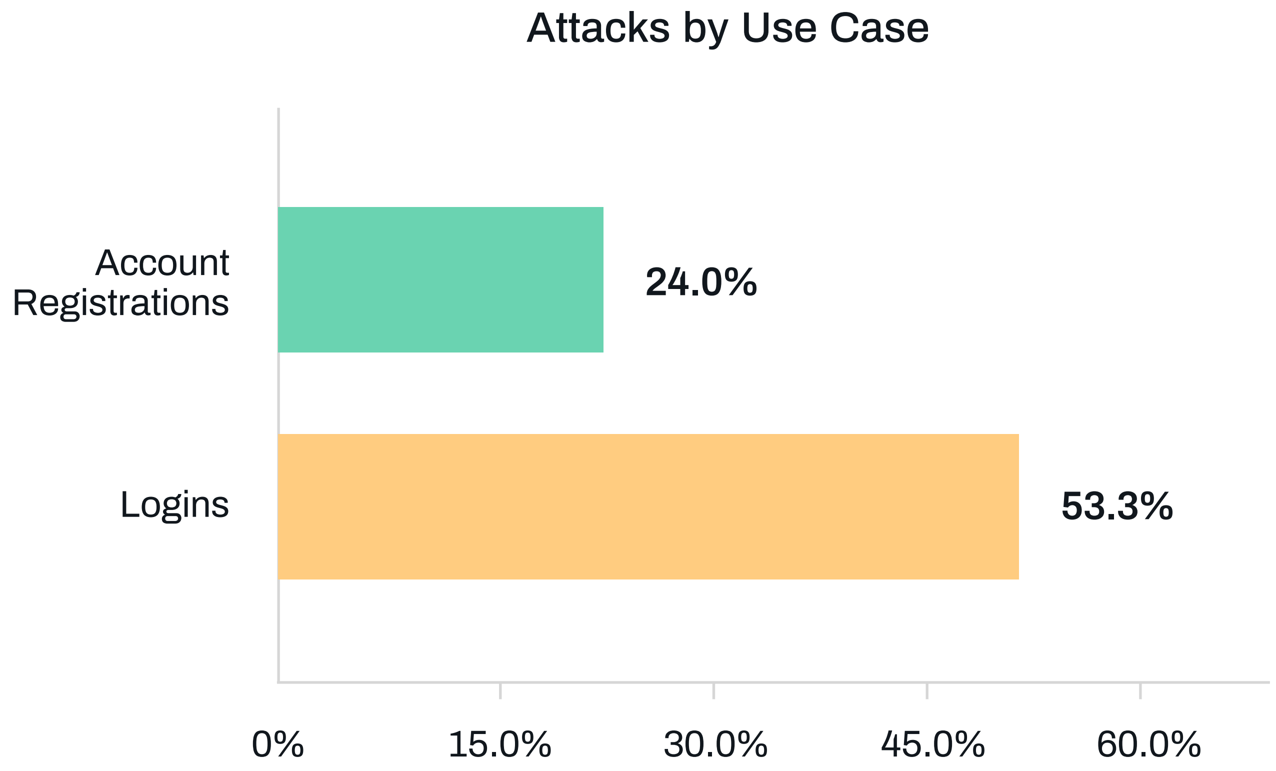
Social Media Transaction Analysis

Social media platforms have truly become key in today's digital economy. Because consumers use these platforms to connect with others, share personal information and opinions, make buying decisions, consume information and make recommendations, social media platforms are becoming increasingly influential in the digital economy. As such, these platforms have become a key component of global businesses' digital strategy.

It is no wonder that social media platforms are lucrative targets for fraudsters looking for quick monetization. From account takeover attacks to fraudulent account creation attacks to spam and abuse, social media platforms see all kinds of attacks from both bots as well as organized malicious humans.

Logins are the biggest use case, as can be expected from digital first companies with strong focus on customer engagement. Unlike other segments, account takeover attacks are more common for social media with logins twice as likely to be attacked than account registrations. This is driven by the fraudsters looking to harvest rich personal data from accounts of legitimate customers. One unique aspect of account origination attacks is the automated/malicious human mix.





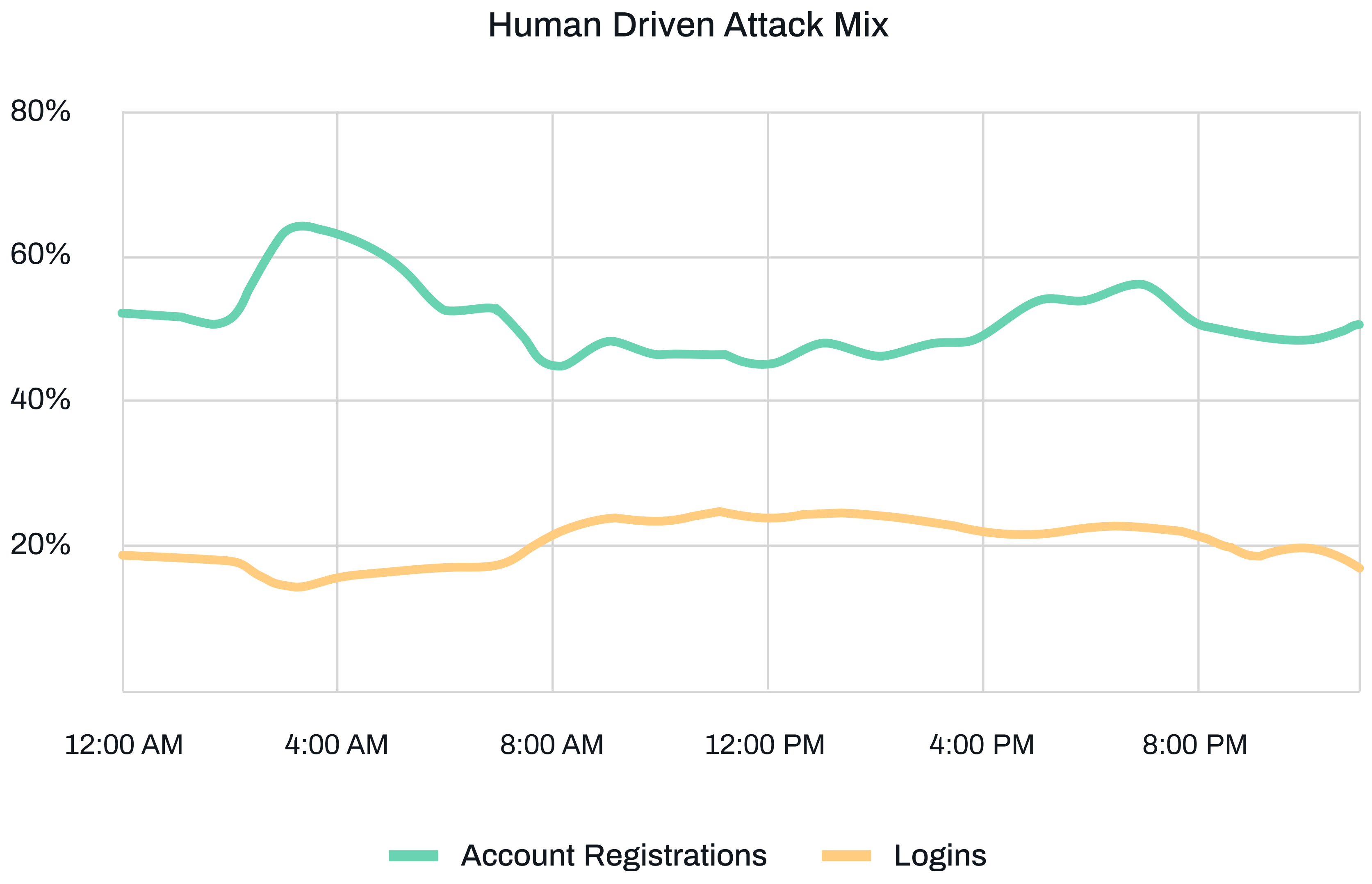
Social Media Case Study - People Driven Abuse in Online Dating

In the new digital norm, social platforms have become central to one's digital journey - for networking, keeping in touch with friends, or to meet potential partners.

These platforms are under constant attack from fraudsters using both bots and organized human sweatshops.

Although login transactions are attacked more, account registrations have a higher mix of human driven attacks. While this may be counterintuitive, this is highly representative of the interactive nature of account registration use case that is geared to catch automation.

To break down the economics of the human driven attacks, fraudsters are presented with a series of challenges that are easy to solve but add up in costs over time, resulting in an increase in the cost per attack.

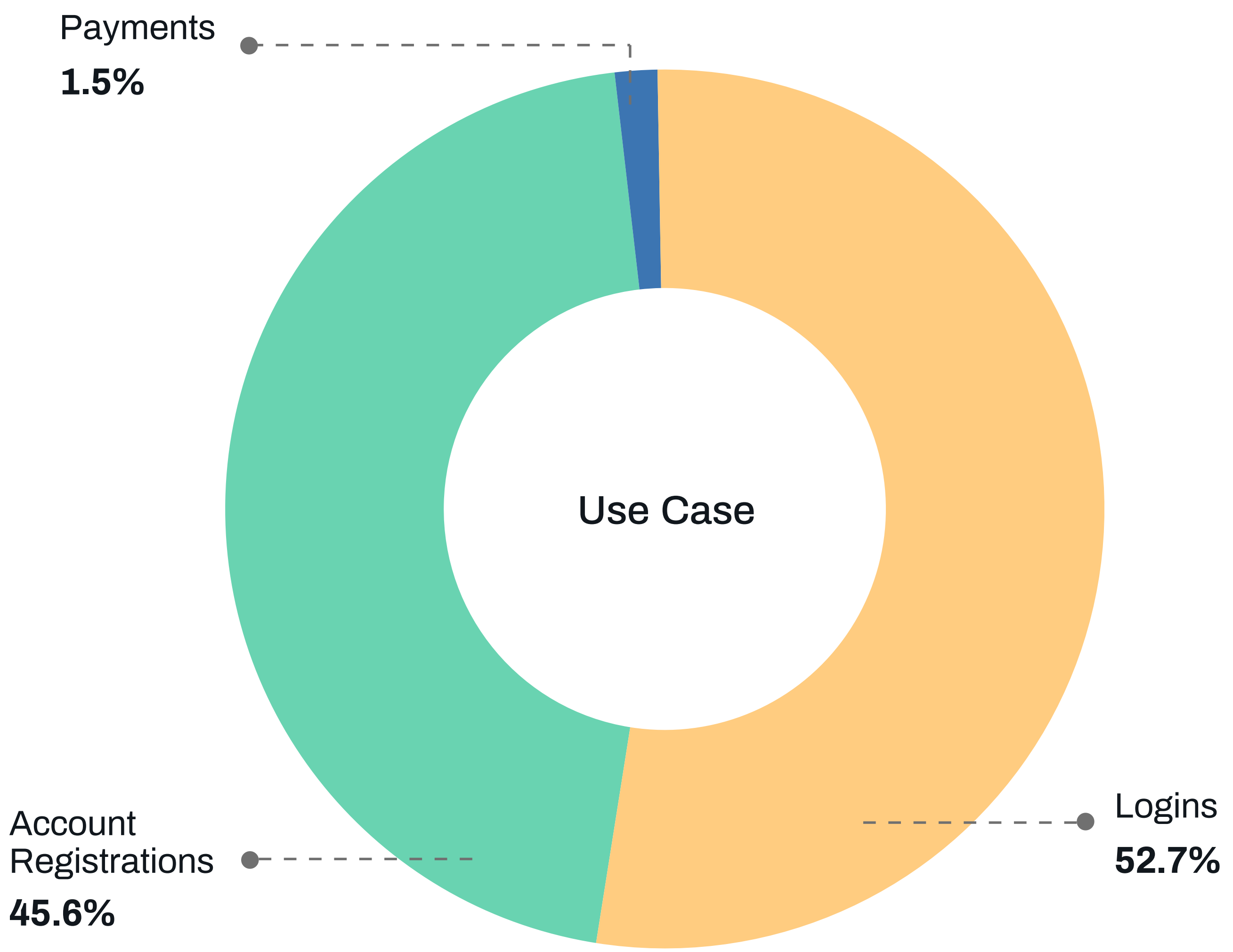


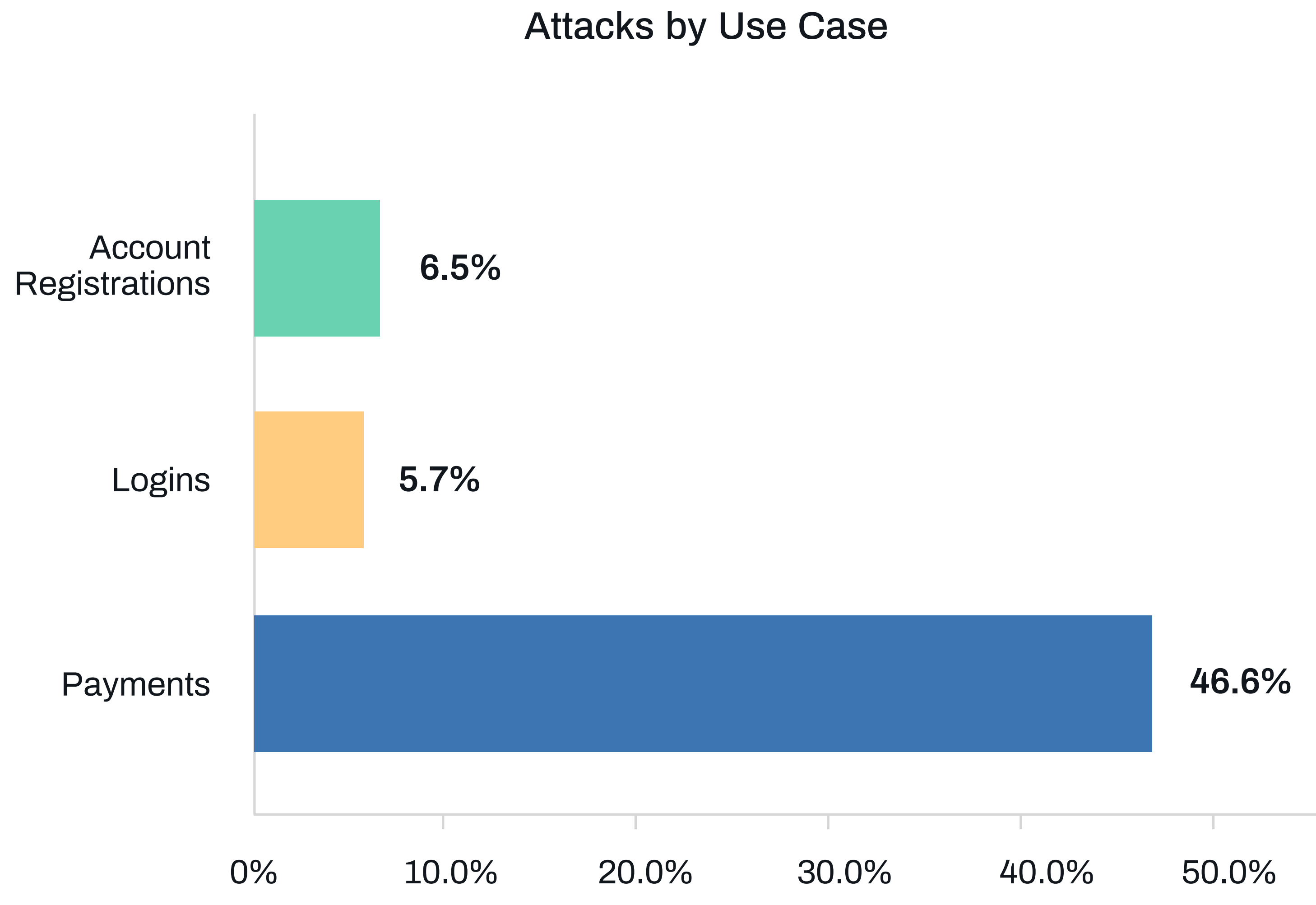
Retail and Travel Transaction Analysis

As travel and retail have moved to the digital channel, so has fraud. One of the key areas of attack growth is seen coming from automated bots that target retailers and travel portals across the globe.

These attacks range from making purchases using stolen credentials to account takeover attacks focusing on loyalty fraud to seat holding attacks on airlines. With each successful attack, consumers either face a significantly increased cost per ticket or lose their valuable, hard-earned loyalty points to fraudsters who took over their accounts.

Payment transactions are 10X more likely to be attacked, especially from automated bots looking to block inventory, leading to denial of inventory attacks or a significant increase in ticket price.



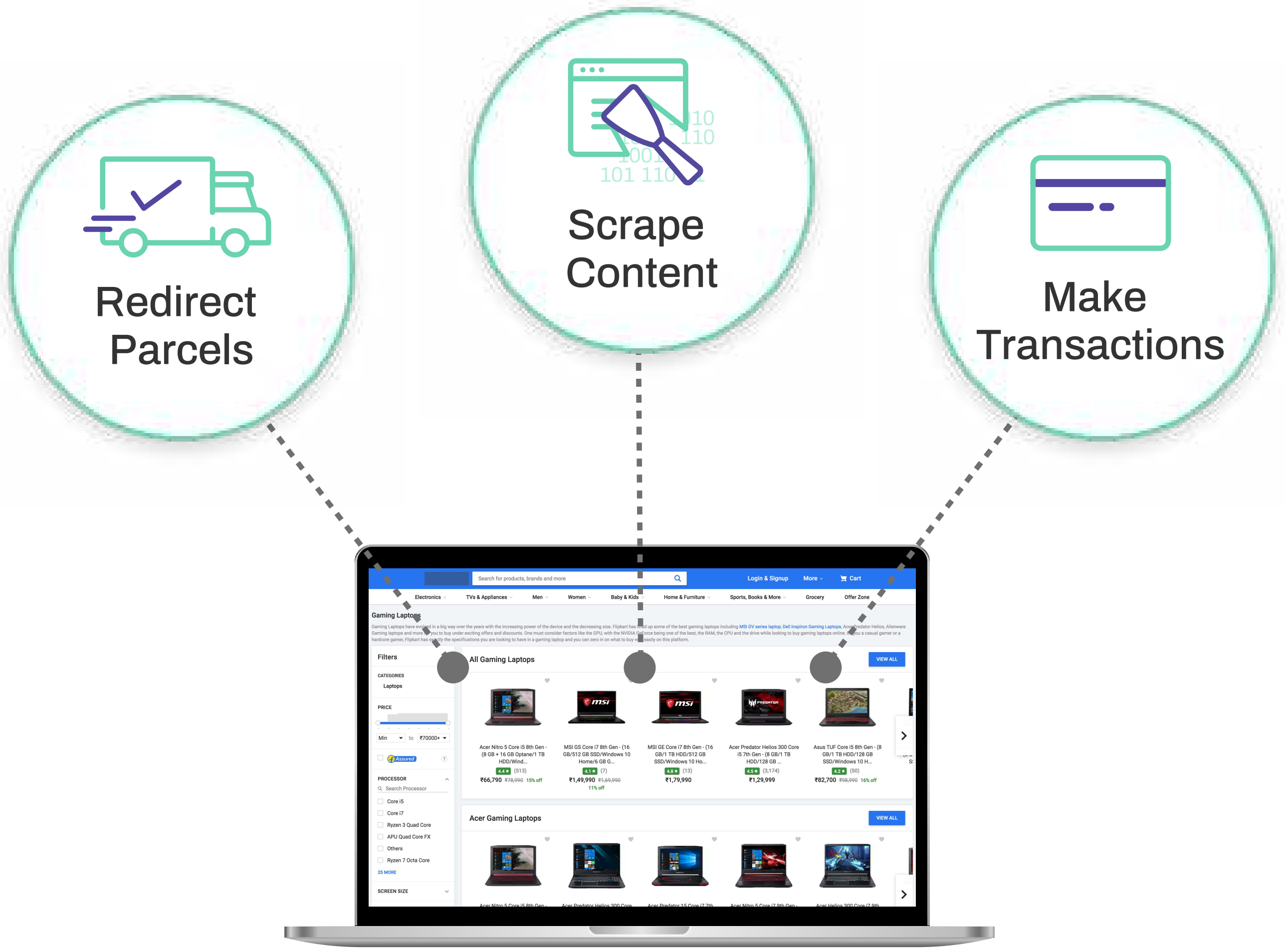


Retail Case Study - Evolving Payment Fraud

Fraud on retailers has evolved beyond payments using stolen credentials that lead to chargebacks.

Retailers across the globe have invested in digital platforms to build close relationships with their customers, offering ‘one click shopping’, targeted recommendations as well as lucrative discounts. This has also attracted fraudsters who try to take over legitimate user accounts to either redirect delivery, make account updates or scrape content.

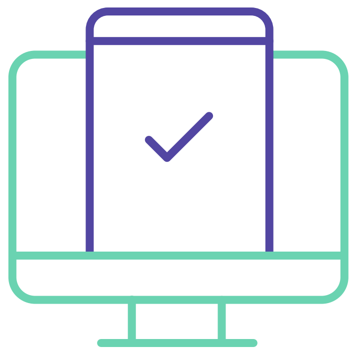
For the digital economy, identity is the real currency, which is truly evident in the retail segment.



Travel Case Study - Denial of Inventory Attacks on Travel

The fraud and risk landscape is rapidly evolving with fraudsters trying to devise novel ways to attack businesses and monetize their operations. This is especially true for travel and ticketing space where the attacks go beyond traditional payment fraud.

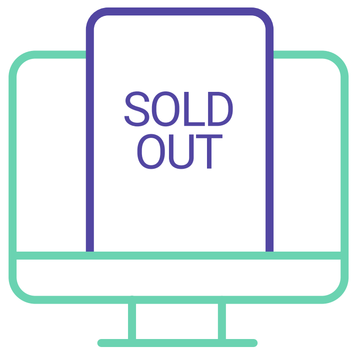
One such emerging attack type is the automated denial of inventory attacks on ticket reservations. For travel, the inventory being held by attacks, triggers cost increases on the remaining seats, or exhausts the inventory on low-cost airlines. This forces consumers to consider purchasing from more expensive alternatives. For event ticketing, bots can book tickets to popular events and sell them at a premium, negatively impacting the overall experience for good customers.



Bot reserves
seat selection

Uses payment
redirect option

Doesn't transact,
holds reservation



Humans can't book
any available seat

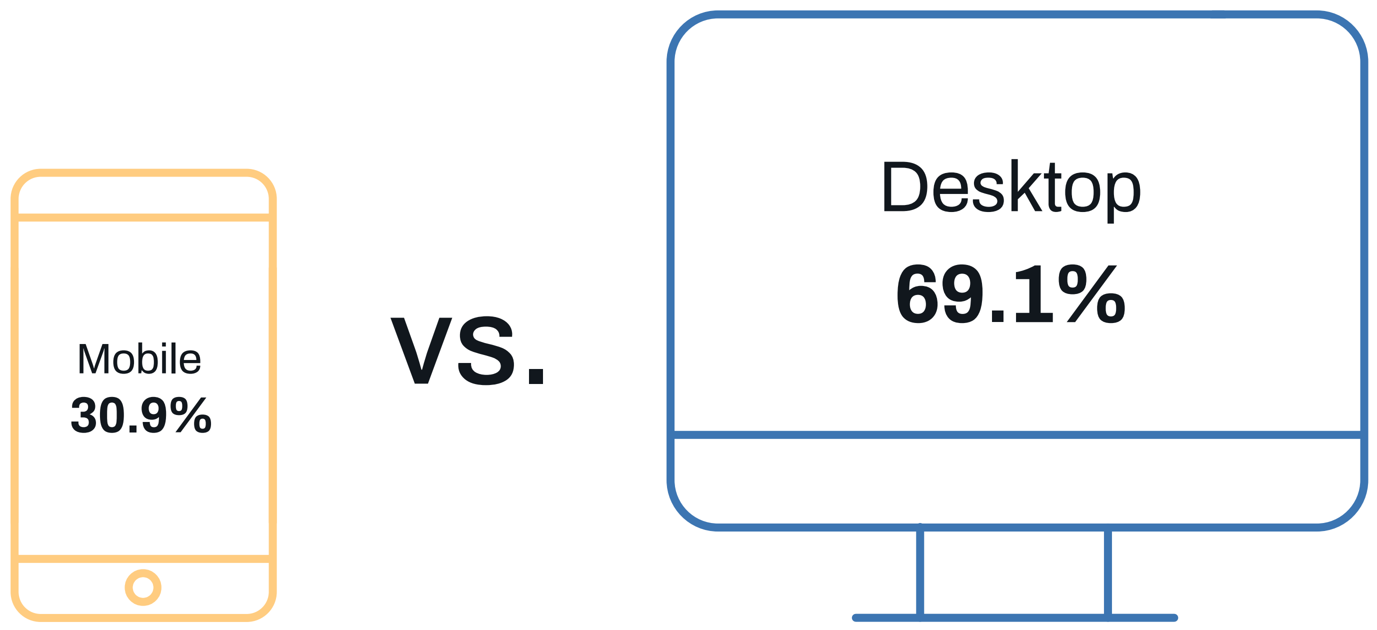
Mobile vs. Desktop Transaction Mix

About 30% of all sessions originate from mobile devices, with the rest coming from other connected devices including laptops and gaming consoles.

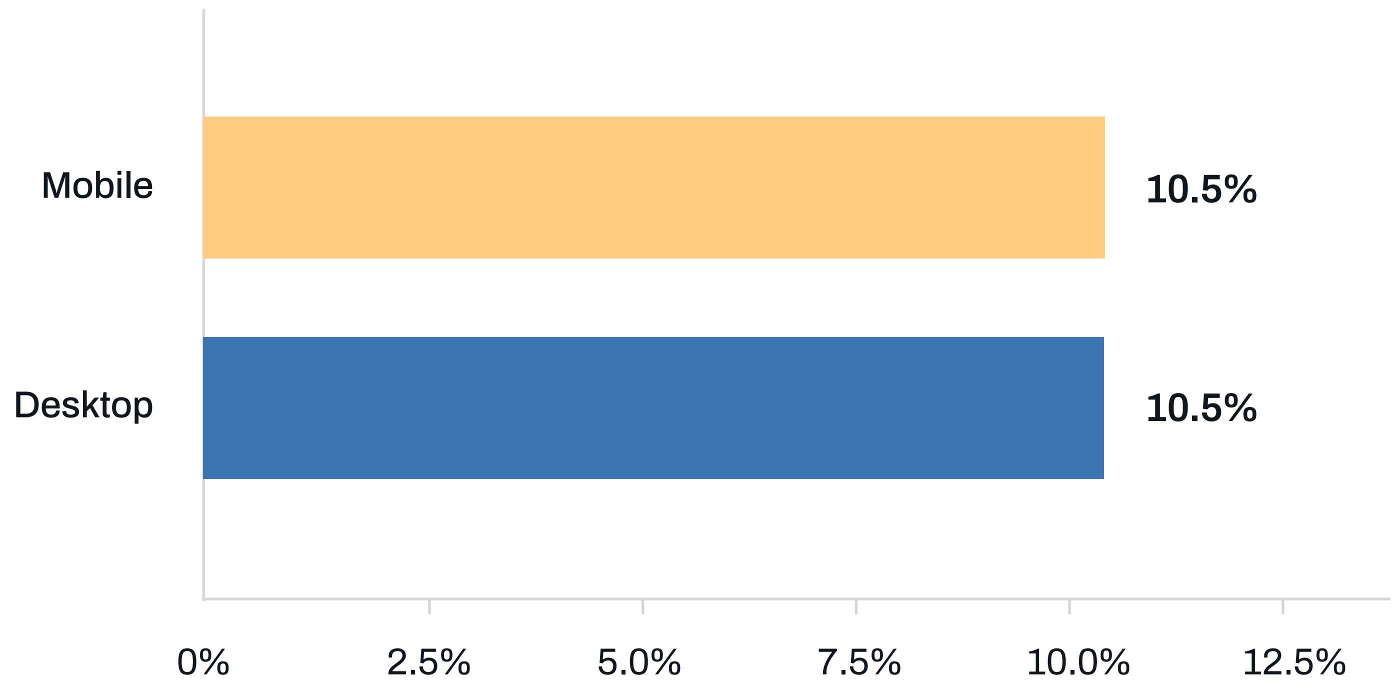
The mobile vs. desktop mix varies by industry with more than 50% of the traffic coming from mobile for social and retail, and a high mix of traffic from consoles in the gaming vertical. On the other hand, finance and tech traffic is primarily web owing to the convenience of the larger screen.

The popularity of mobile is now evident in the attack mix. During the early days of mobile commerce, organized attacks primarily targeted web traffic, owing to low volumes. However, with the adoption of mobile, especially in emerging economies, fraudsters attack mobile traffic just as much as the web traffic.

Transaction Mix



Attacks by Channel



Conclusion

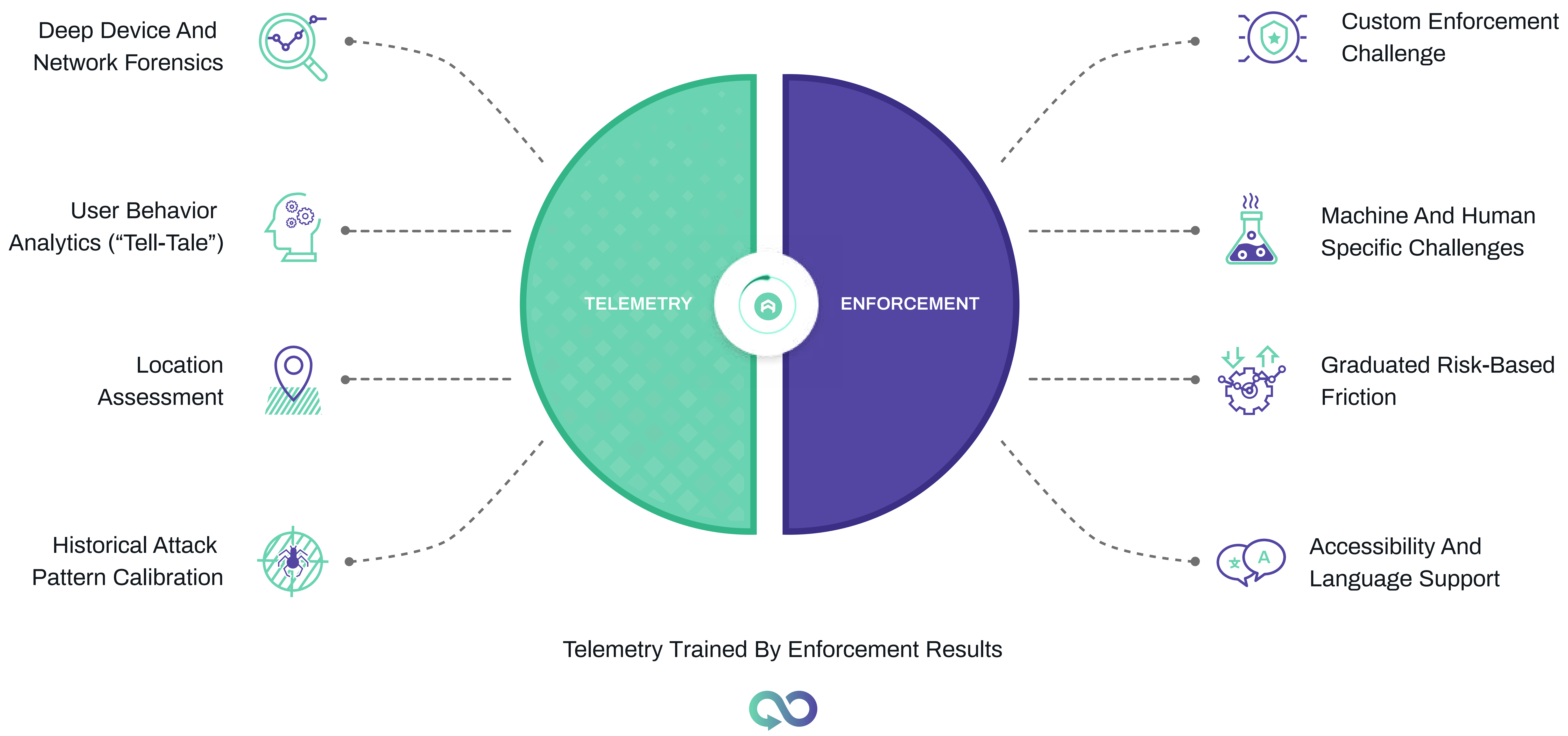
This report further reinforces that today's digital environment is giving way to new and sophisticated security threats. Fraudsters have the tools, resources and financial incentives to find ways to attack digital businesses for quick financial gains. Automation is fueling the scale and impact of online fraud and automated attacks are more prevalent than ever before.

We are entering an era where online identity, intent, business, metrics and content can all be faked, while the good user behavior can rapidly evolve. This can have serious security and financial repercussions for any business with an online presence, especially as they try to balance risk management with delivering exceptional customer experience.

As the businesses focus on deploying tools to stop attacks, fraudsters look for ways to bypass those defences. Each successful attack further provides funds and resources to the fraudsters. It is important now, more than ever to approach this problem by understanding the fraudsters' business.

Arkose Labs believes that combating the growing online fraud epidemic requires a solution rooted in prevention and stopping of abusive attacks at the point of entry without disrupting user experience. Making the attacks more difficult and costly disrupts their economic incentive and breaks their business model. This results in a longer term solution and stops the cat and mouse game that fraudsters play with businesses.

Arkose Labs Fraud and Abuse Prevention 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.
- User sessions: Customer interaction/transaction including logins, account registrations and payments.

Telemetry and Enforcement

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

Fraud Types (cont.)

- Gift Card Fraud: Numerous ways of stealing money off the gift cards.
- 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

- Automated Attacks: Large scale attacks using BOTs and other sophisticated tools.
- Human Driven Attacks: Sweatshops/Clickfarms employing a large group of low-paid workers to launch attack or make fradulent transactions.
- Single Request Attack: A technique where breached email addresses are automatically matched with the top most common passwords to facilitate account takeover.

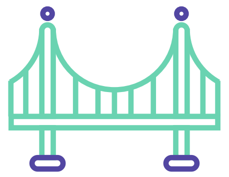
About Arkose Labs

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