Arkose Labs

Fraud & Abuse Report | Q3 2020

Data-Driven Analysis of 2020 Fraud Trends

Introduction - The Long Tail of COVID-19

The digital commerce landscape has fundamentally changed since the beginning of 2020. Digital natives have been joined by a wider demographic, who flocked to digital channels during COVID-19 lockdowns. There has been a blurring of the online and offline world, as traditional stores turn to technology to minimize physical contact between customers and staff and increase reliance on online orders and BOPIS*.

Understandably, this is having a direct impact on the fraud threat landscape. Businesses are operating under high-pressure scenarios and incentive levels for would-be fraudsters are sky high. We see heightened attack rates, significant spikes in fraud attempts and greater volatility than in 2019.

Fortunately, fraud departments have been adjusting well to work from home models and the businesses we speak to are continuing to prioritize strategic fraud technology investments - even in industries seeing drop offs in consumer traffic due to COVID-19, such as travel.

This report looks at top global trends since the beginning of 2020 and unveils key industry insights from the last quarter. By better understanding the evolving digital landscape, businesses can ensure they are well-equipped to tackle the rising tide of fraud and ensure long-term protection against attacks.

**BOPIS: Buy online pick up in store*

By better understanding the evolving digital landscape, businesses can ensure they are well-equipped to tackle the rising tide of fraud and ensure long-term protection against attacks.

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 June 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 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 '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 for the purposes of this report.

1H 2020: Key Fraud and Abuse Trends

As COVID-19 forces commerce online, the Arkose Labs network records double the volume of attacks over 6 months.

1.1 billion
attacks detected and stopped

2x attack volume
since 2H 2019

25% attack rate
on all transactions

Elevated Attack Levels in 2020

Attack patterns have been evolving rapidly in the first 6 months of 2020

21.2% mobile
attack mix

33.5% human
vs 66.5% bot attacks

Most attacked
use case is logins

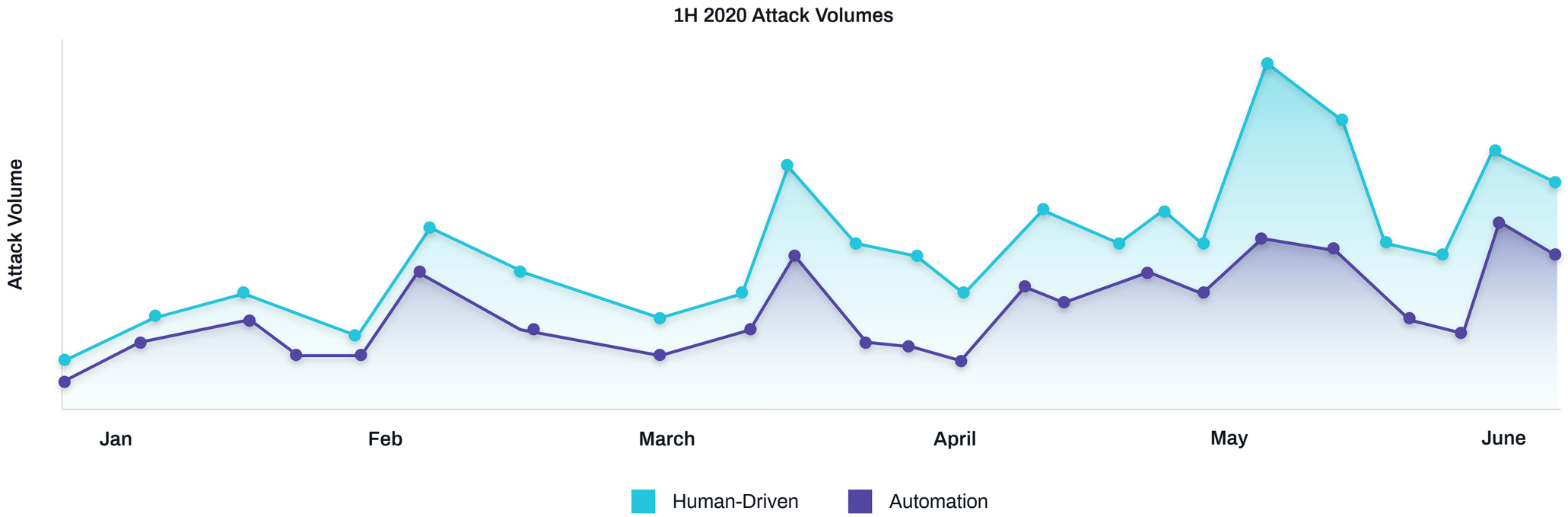
Gaming industry
sees most intense attack levels

65 attacks per second
for gaming industry

Heightened Attack Volumes in 2020

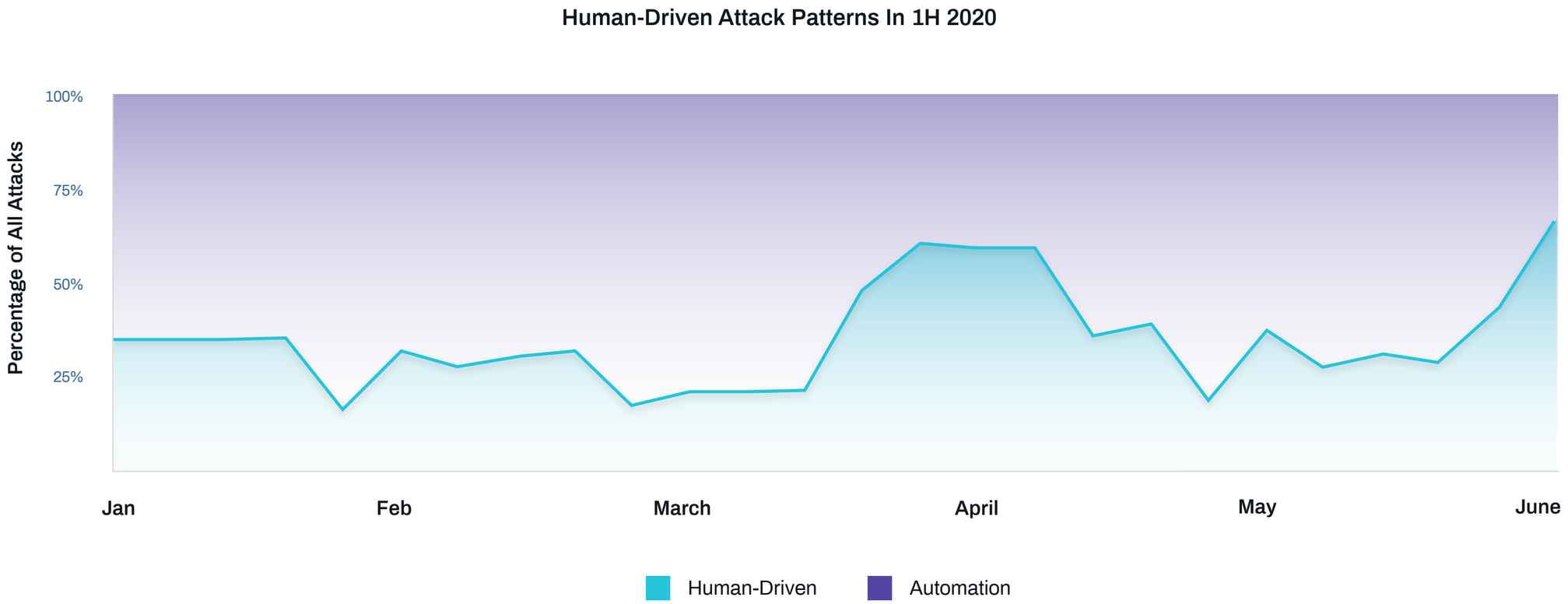
Businesses are facing an increasingly hostile threat landscape in 2020. Major spikes in attacks can be seen across the first six months of the year, and Arkose Labs has observed a general upwards trend in the intensity of attacks. Normal consumer behavior has been in flux, due to the upheaval caused by COVID-19. It is harder to user historical benchmarks of transaction habits when assessing traffic.

Therefore, organizations relying purely on data-driven fraud defenses run the risk of more traffic falling into a "gray area" when differentiating between trusted and fraudulent behavior. They therefore require robust defenses that provide hard evidence of a user's true underlying intent.



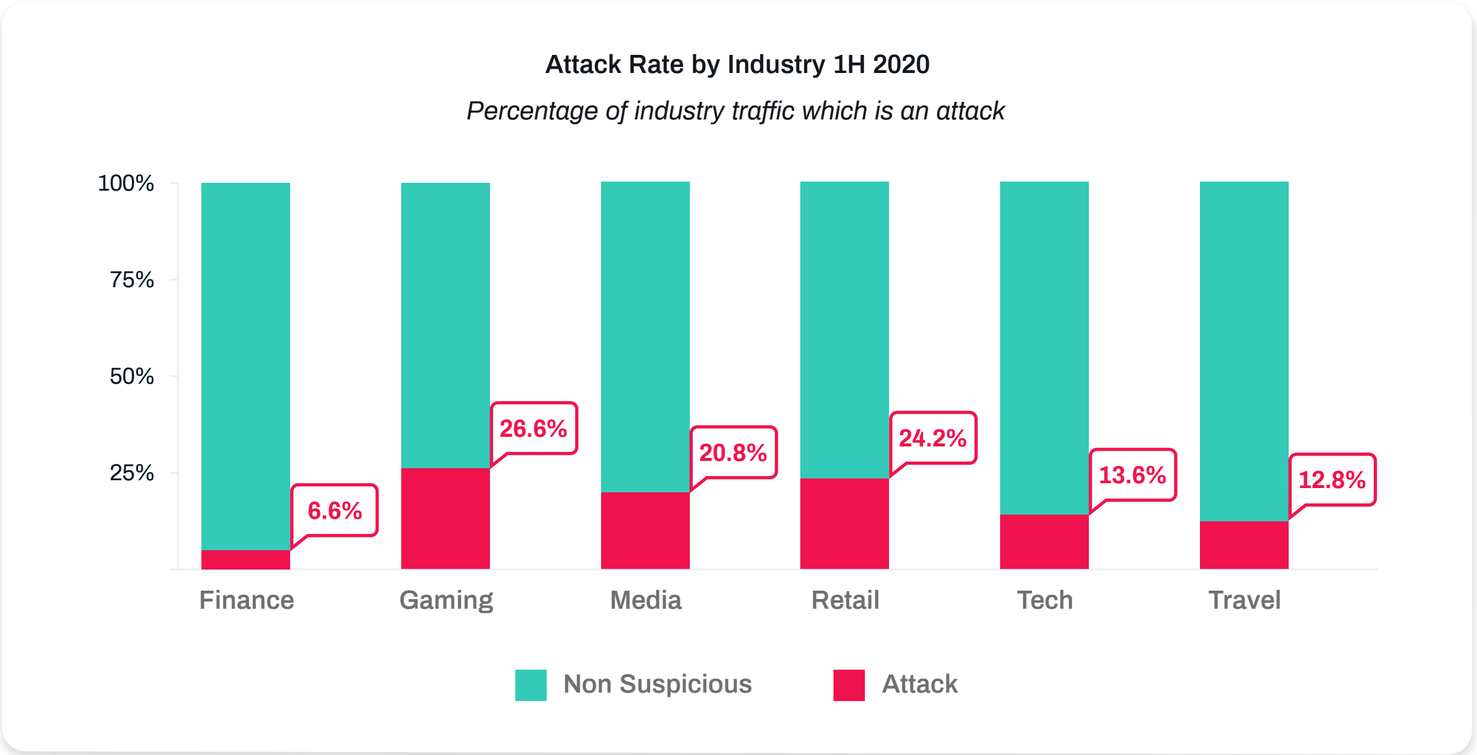
Human vs Bots: Hybrid Attacks are Becoming More Prevalent

2020 has witnessed constant volatility in the human versus automated attack mix. Bots were largely driving spikes in attacks in the first quarter of the year, with fraudsters pivoting quickly to augment attacks while digital transactions spiked amid COVID-19 lockdowns. Sweatshop attacks have since ramped up and were very active by April. More and more attacks use a combination of human and bot resources. The Philippines is the country with the highest human-driven attack volumes, along with Russia and the Ukraine.



Gaming and Retail are Top Target Industries in 1H 2020

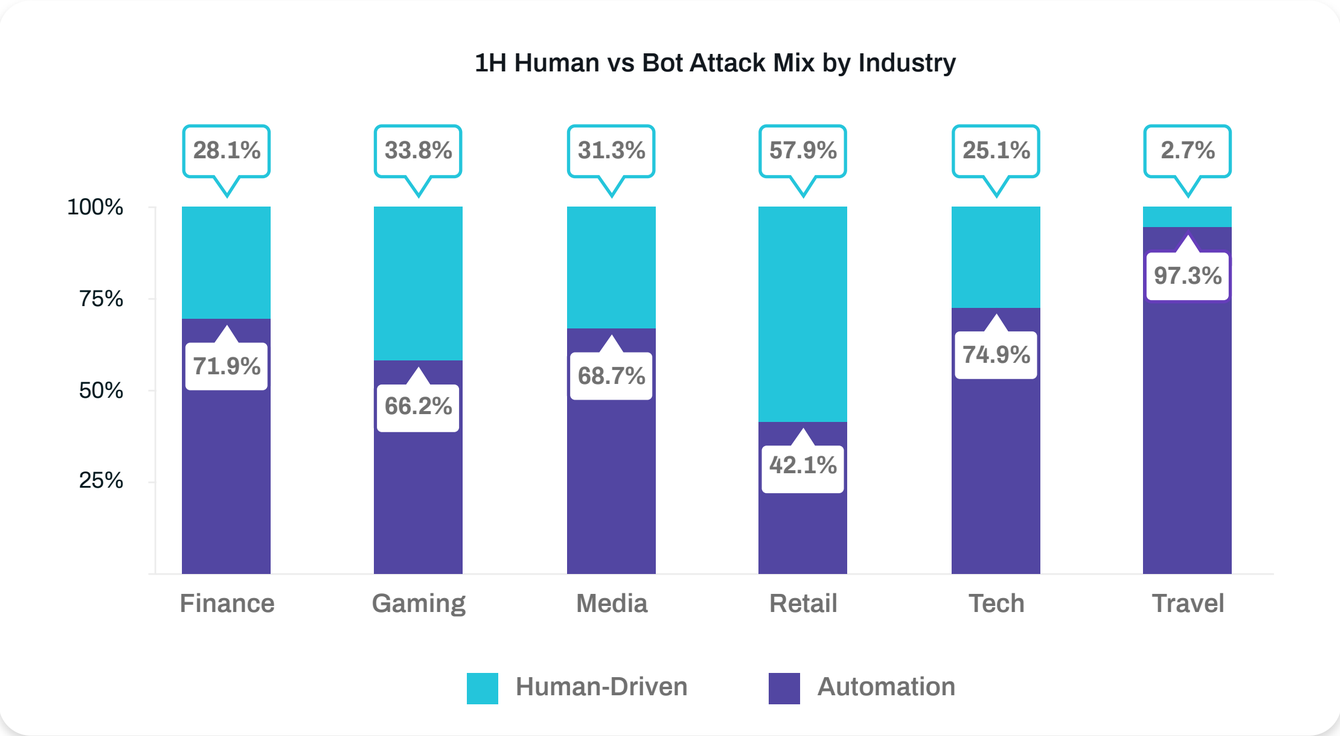
Gaming and retail have the highest attack rates in the first half of 2020 - a quarter of all traffic represents an attack for these industries. These are the two industries with the biggest uptick in consumer traffic amid lockdowns, as face to face transactions are restricted or discouraged. With adults and children confined to their homes, people have become very active on online gaming platforms. Fraudsters follow these trends closely and will target businesses at times of high traffic, attempting to blend in with good users.



Major Variations in Attack Mix Across Industries

The amount of time and effort that a fraudster is willing to expend on an attack is driven by the monetization potential. As human-led efforts are always a greater investment for attackers, it is revealing to monitor the proportion of human-driven attacks versus automated bot activity targeting industries.

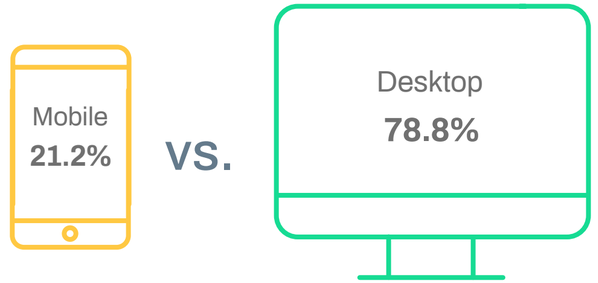
The highest human-driven attack rate is in retail over the first 6 months of 2020. At the other end of the spectrum, human resources were expended very sparingly on travel companies, which have been suffering from a major drop in customer activity due to travel restrictions.

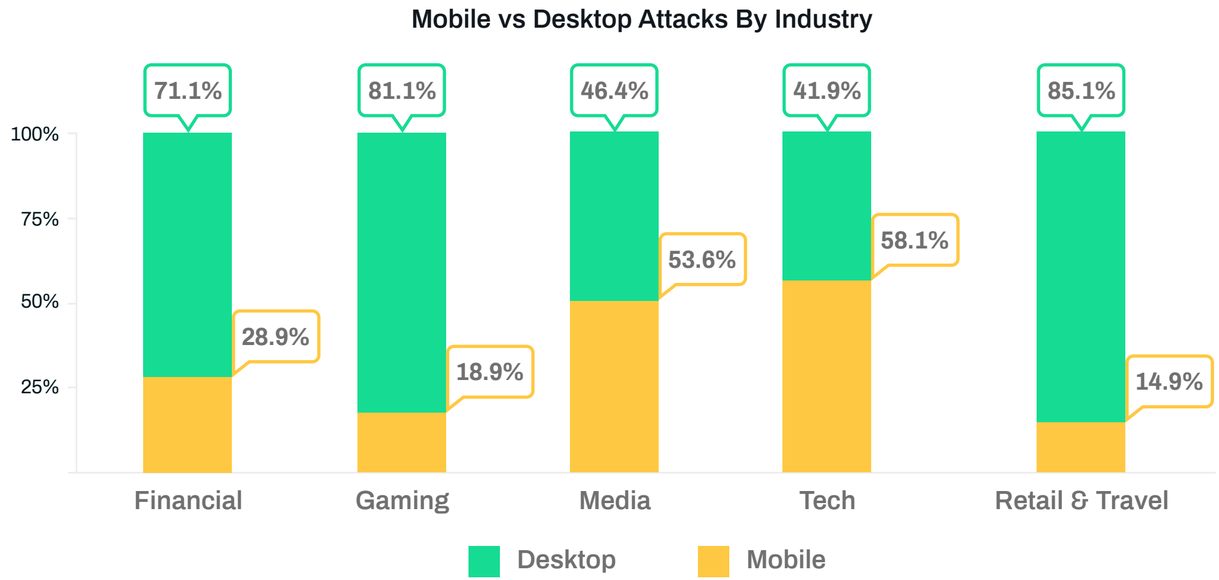


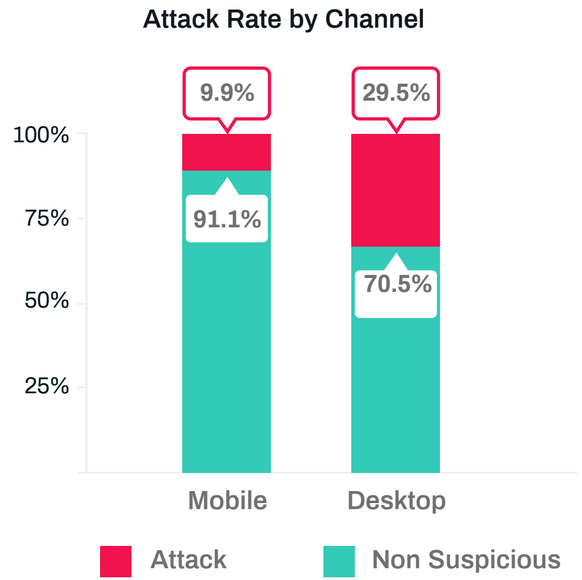
Mobile Powers Sweatshop Attacks

While mobile attack rates vary greatly by industry, overall they are lagging behind desktop attacks on the Arkose Labs network. 37% of all transactions originated from mobile, but only 21% of all attacks were on mobile transactions. Of those mobile attacks, 38% were human-driven which is higher than the overall human-driven attack mix. Click farm workers will line up multiple mobile devices to execute attacks at scale.

There is a great deal of variation in the mobile versus desktop attack mix when parsing this by industry. Media (including social media) and technology saw a majority of their attacks targeting mobile transactions.

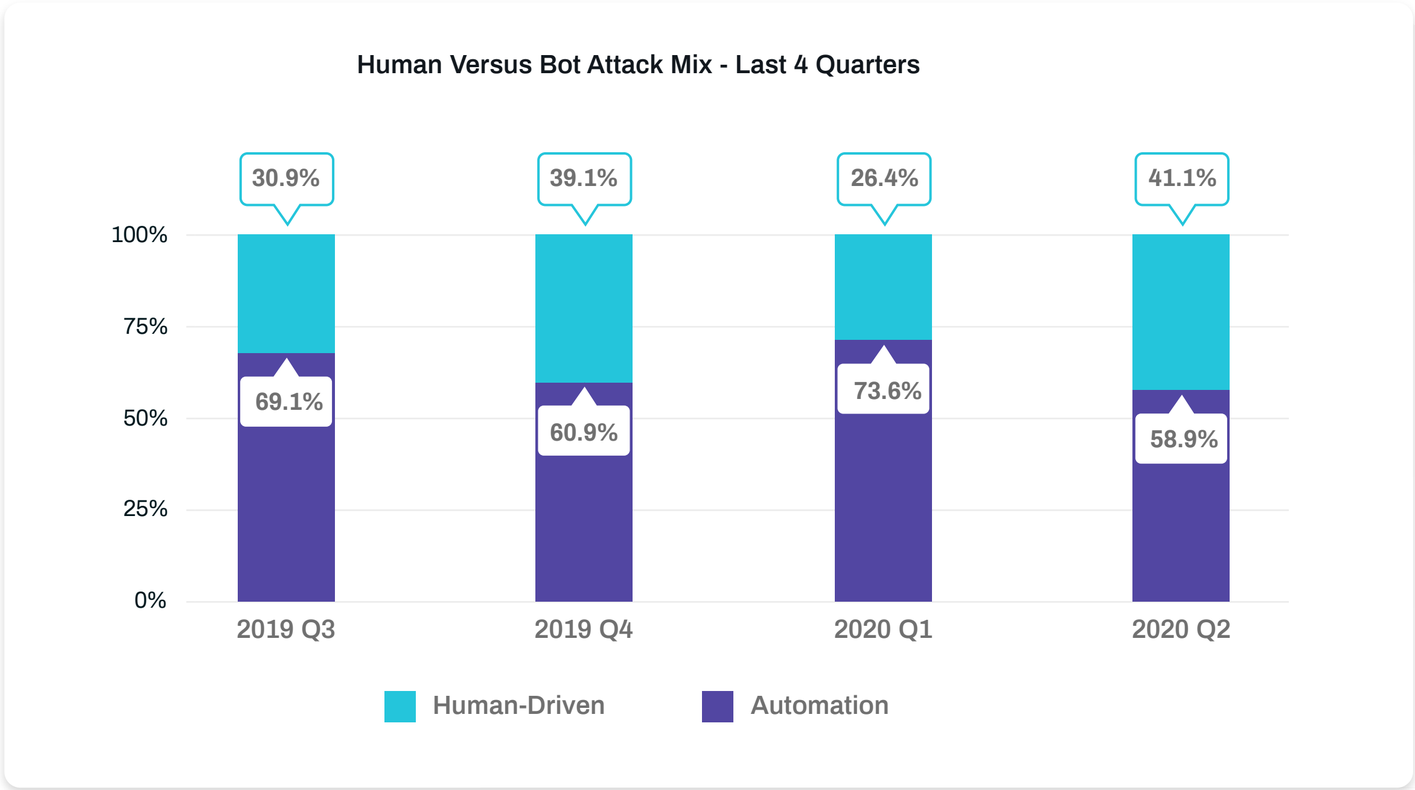






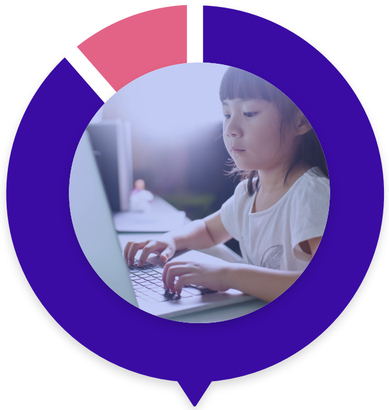
Human Versus Automation Attack Mix

This graph demonstrates that the overall human versus bot attack mix does generally vary from quarter to quarter. Fluctuations occur as customers on the Arkose Labs network deflect different organized attacks. Q1 2020 saw a barrage of bot attacks, which represented 74% of all attacks. Whereas, the most recent quarter saw the highest proportion of human-driven fraud recorded over the last twelve months, with 41% of attacks originating from sweatshops and other malicious humans.



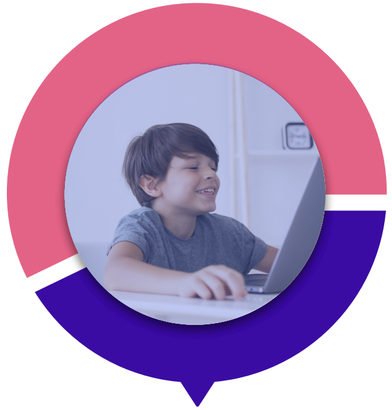
COVID-19 Lockdowns Accelerate Digital Adoption Among Kids

COVID-19 lockdowns across countries have forced closures of schools, daycare and other institutions. A lot of teaching activity is now being done through digital means, either using video conferencing tools or videos that teachers create and upload to an online repository. Furthermore, social interactions are also happening more frequently online for children. These can take the form of the “zoom playdates” that have become commonplace during lockdowns. Additionally, children are spending increasing hours on digital entertainment platforms.



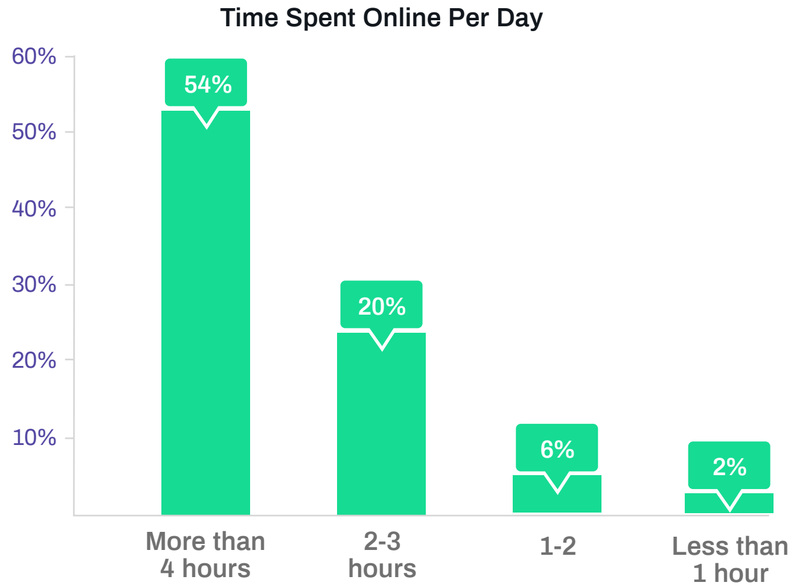
95%

of children spend more time online due to COVID-19



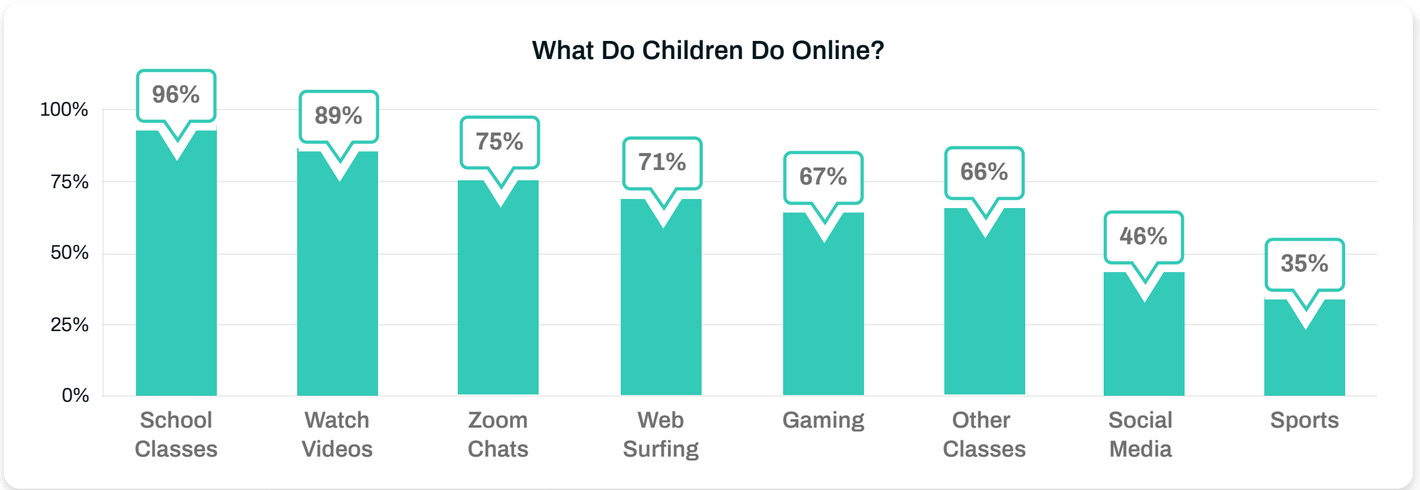
44%

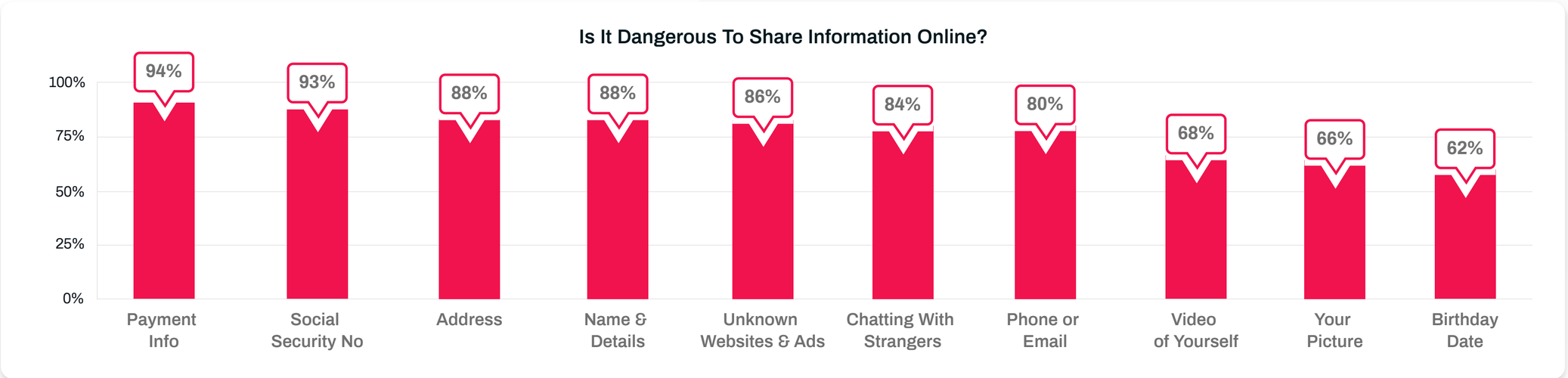
of children careful sharing information online



Today's Users; Tomorrow's Spenders

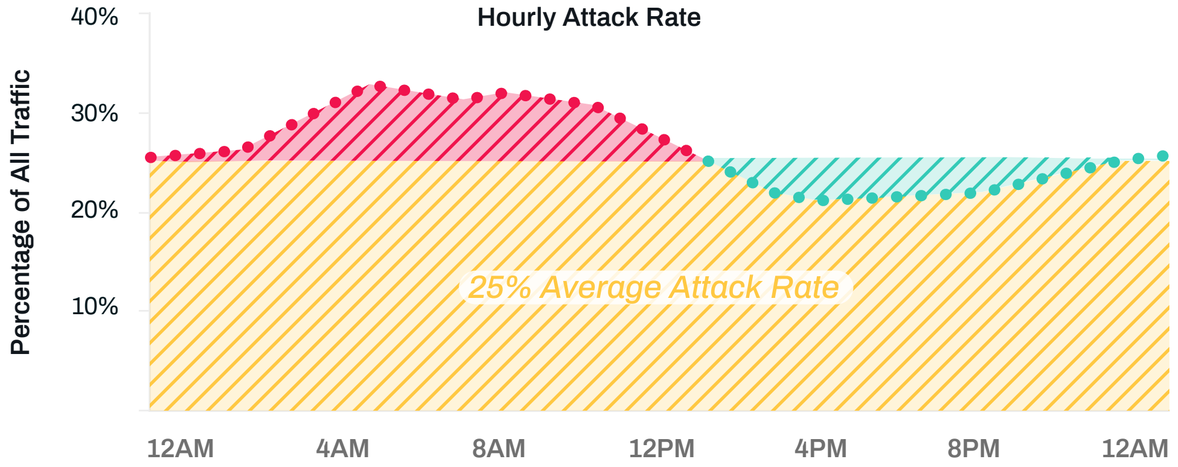
Arkose Labs surveyed children across the globe on their digital habits in 2020. The effect of COVID-19 was very much apparent, with classes for school being the top online activity. There was a high awareness of the dangers of sharing payment information online, however the dangers of sharing personal data such as birthdate was much lower ranked by the children in the survey.





The Most Dangerous Hour of the Day

When comparing attack levels with legitimate traffic patterns, it is clear that the morning is most dangerous period of the day. Businesses are facing cross-border attacks from fraudsters operating across timezones and using automated scripts that can run through the night. Therefore, attacks do not always tie in with the peak hours of legitimate consumers. 5am is the time of the day that has the highest attack rate across all traffic, with attacks 10% higher than in the afternoon. Traffic coming between the hours of 4am and 10am is generally higher risk than other times during the day.

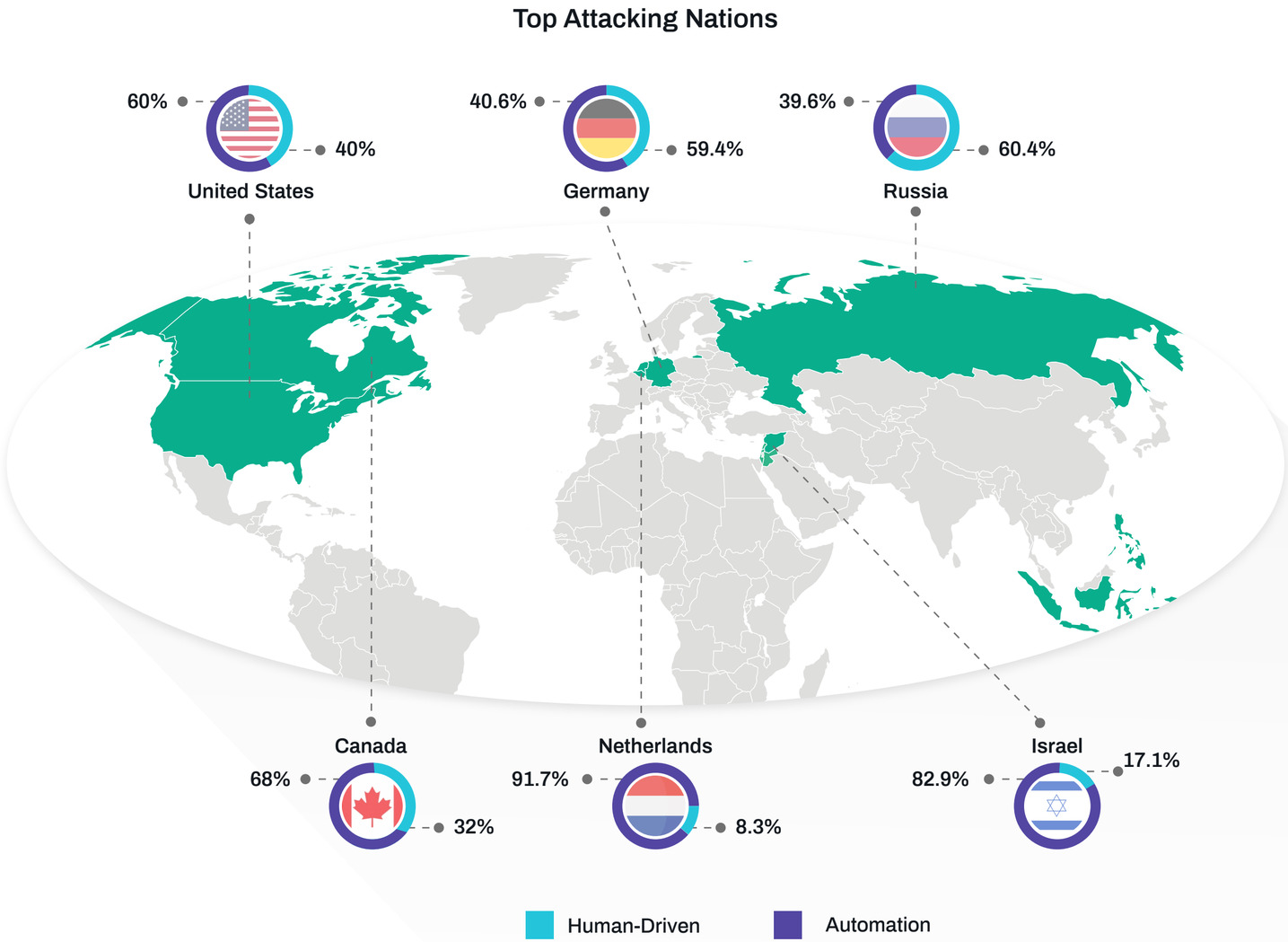


Highest attack rate at 5am

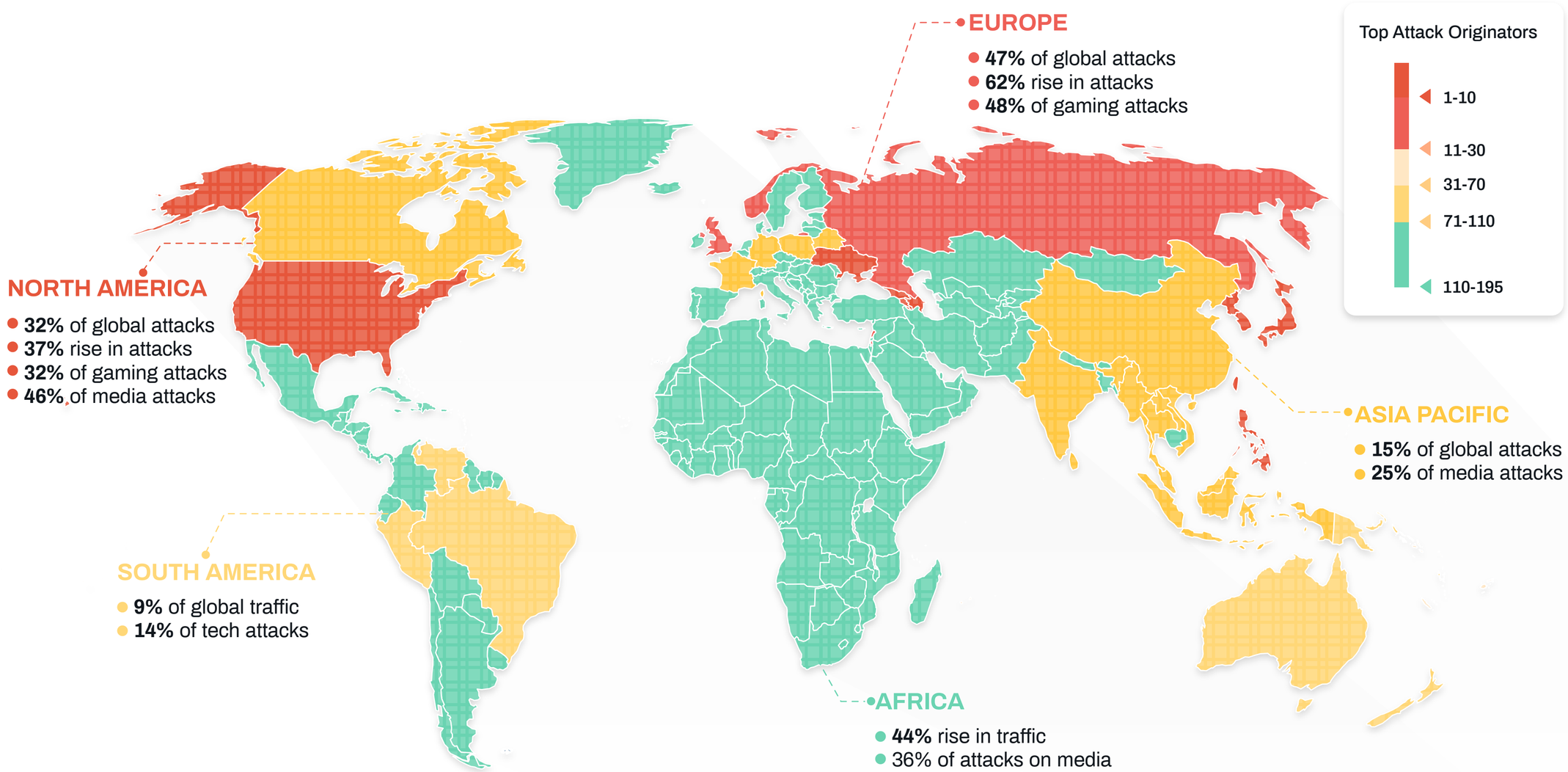
Elevated attack rates between 4am and 10am

Top Attacking Countries in Q2 2020

In Q2 2020 there was a surprising dominance of more well-established economies among the top attacking nations, rather than traditional fraud hubs in developing economies. This could be attributed to COVID-19 lockdowns, with the allure of fraud now more widespread. In times of economic hardship, there are increased incentive levels for would-be fraudsters, even in richer nations, and the cybercrime ecosystem will pounce on new opportunities for recruitment. This demonstrates how quickly organized fraud will mobilize to take advantage of changing economic circumstances.



Regional Attack Patterns



The Tale of Two Fraudsters: Human Drivers Behind the Stats

The proportion of human-driven fraud versus bots rose this quarter with 41% of attacks originating from sweatshops, compared to 59% for bots and automated attacks. This is a significant increase from Q1, when humans accounted for 26% of all attacks.

Low-Skill Opportunism:

There has been a proliferation of services and marketplaces which connect low-skill workers who can help fraudsters carry out digital attacks at scale for very little remuneration. These appeal to people in places with a very low cost of living, where just $100 a month can be an alluring prospect. The attraction of this low-reward activity goes up in times of economic turmoil.

Determined Attacker:

In Q2, a gaming customer faced a dogged attack from a highly motivated fraudster. They attempted to reverse engineer the parameters used in the Arkose Labs platform to trigger enforcement challenges and circumvent authentication steps at scale. Targeted attacks require solution providers to go the extra mile to work with the customer and ensure attacks are not getting through.

41%
Human-driven fraud

15%
Higher sweatshop mix vs Q1

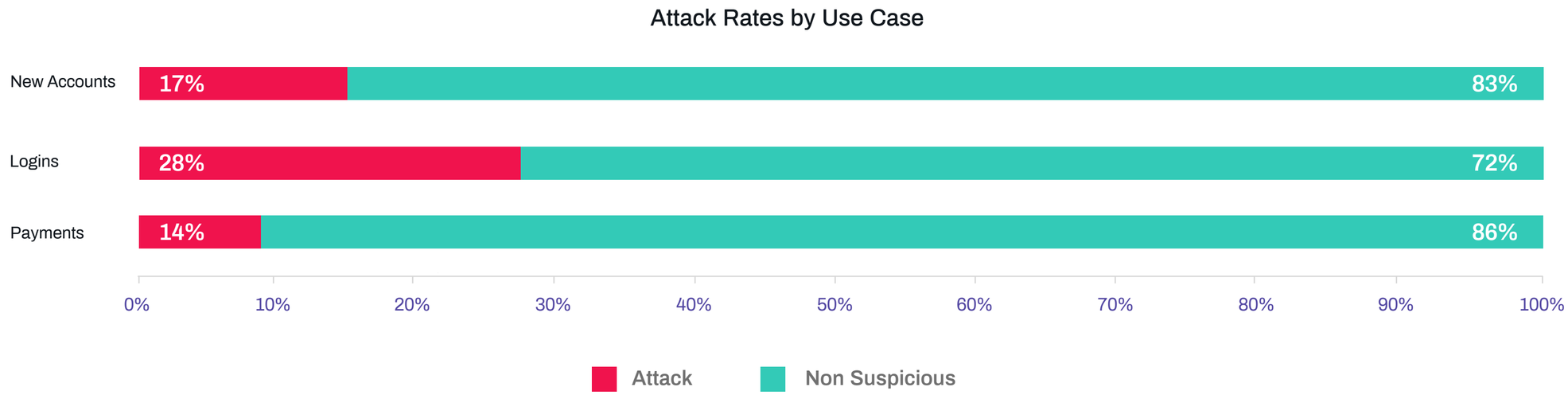
Account Takeover Attempts Most Prevalent in Q2

In the frenzy of fraudulent activity immediately after COVID-19 lockdowns commenced, there were high levels of fraud attempts across all customer touchpoints. The result on the Arkose Labs network was a consistently high attack rate across all the key use cases. This shifted in Q2, when logins was the most attacked touchpoint. The attack rate on logins went up to 28%, which is significantly higher than account registrations and payments.

28% attack rate on logins

30% lower attack rate on account registrations

47% lower attack rate on payments



Media Companies Face Mobile and Sweatshop Attacks

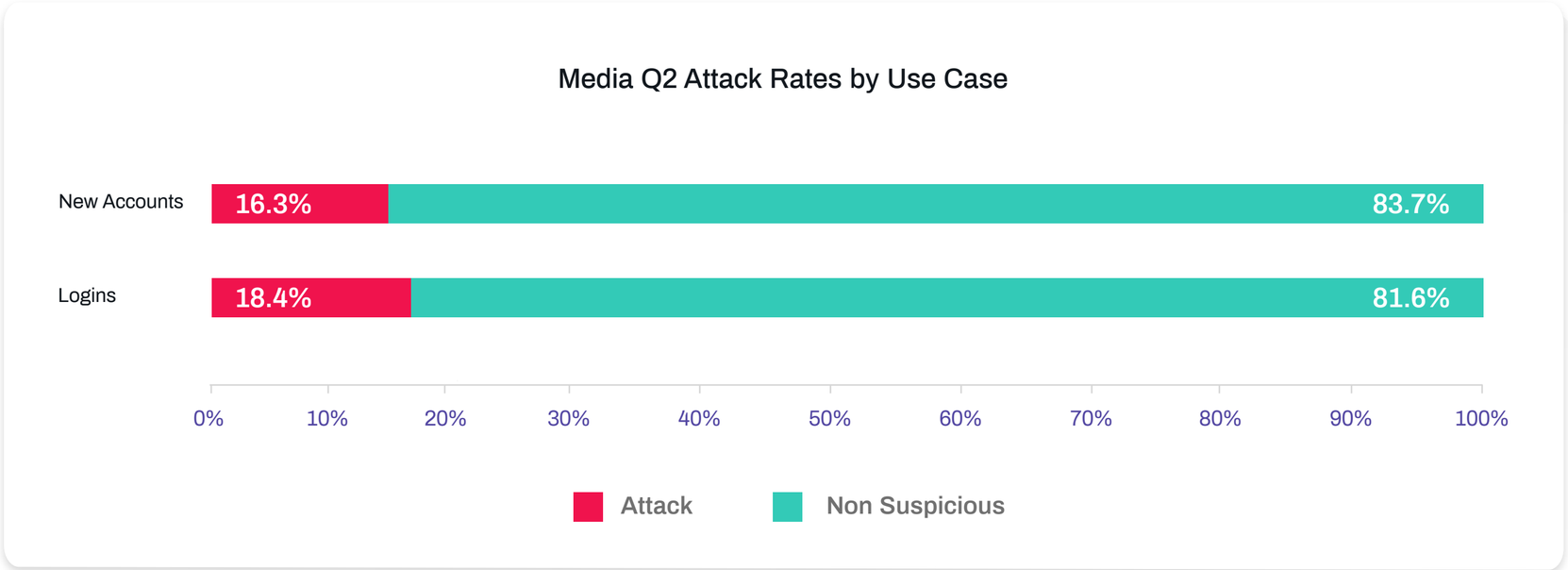
17.8%
attack rate

25.5% of attacks from sweatshops

39% of attacks on mobile

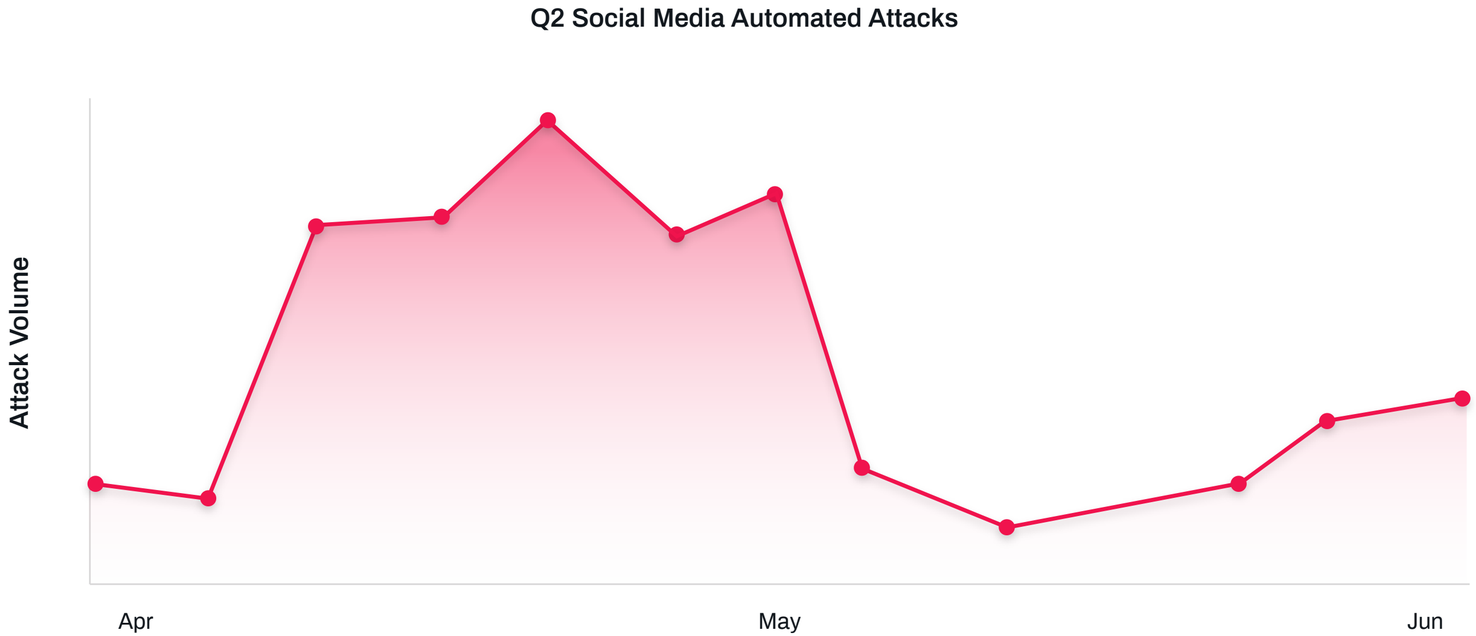
Digital media, streaming and social media companies are major targets for card testing, abuse of free trials and reselling of paid accounts. Without the correct tools in place, companies face major hurdles in stamping out abuse without spending manual time identifying bogus or compromised accounts.

The media industry has high levels of mobile traffic. As a result, it sees elevated mobile attack rates. 39% of attacks targeting media companies are on mobile transactions, which is a higher proportion than any other industry. This was particularly elevated in Q2, with mobile attacks up 31.5% compared to the previous quarter.



The Scourge of Bots in Social Media

Social media sites saw a spike in bot-driven activity in April and May. Bad actors use bots across a variety of social media platforms in order to scrape information, launch scams or disseminate malicious content. Bots are deployed in attempts to influence political and social discourse by spreading information en masse and carrying out hashtag hijacking and trend-jacking. This issue of bots within social media will continue to come under great scrutiny in the second half of 2020, as debates over COVID-19 safety measures and a presidential election in the United States dominate public discussion.



Online Gaming Under Pressure During COVID-19

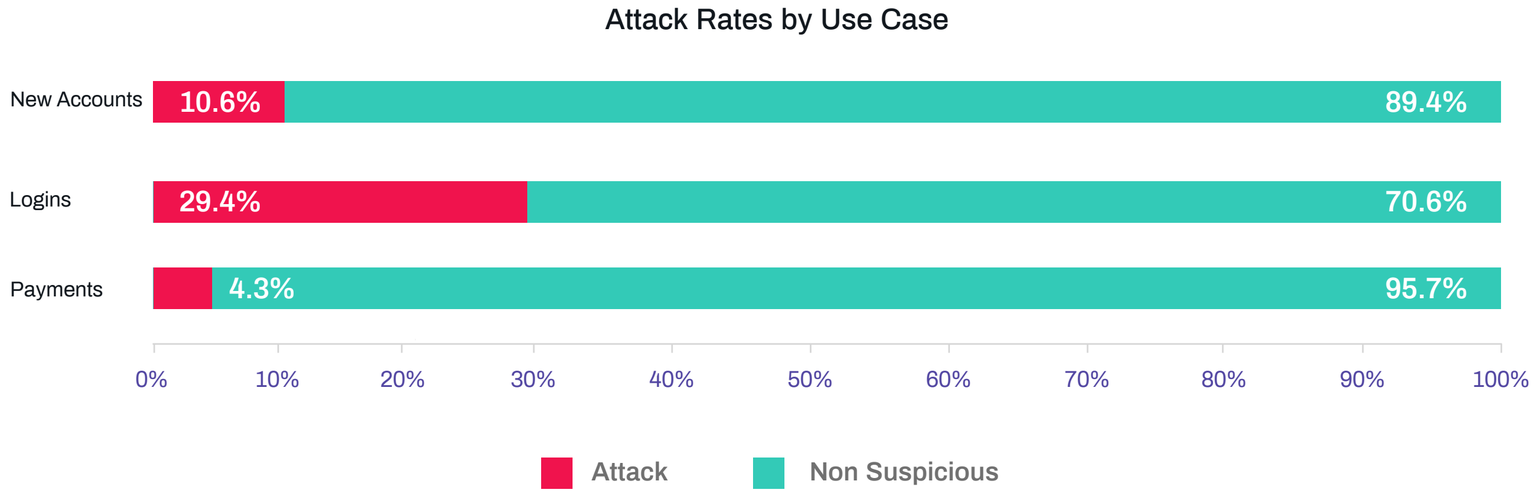
25%
attack rate

41% of attacks from sweatshops

14% of attacks on mobile

Q2 was another busy period for the online gaming industry. With lockdowns still in force and people spending more time at home, gaming traffic rose another 30% compared to Q1 2020. The most attacked touchpoint was logins, which saw a 22% uptick in the volume of attacks versus the previous quarter.

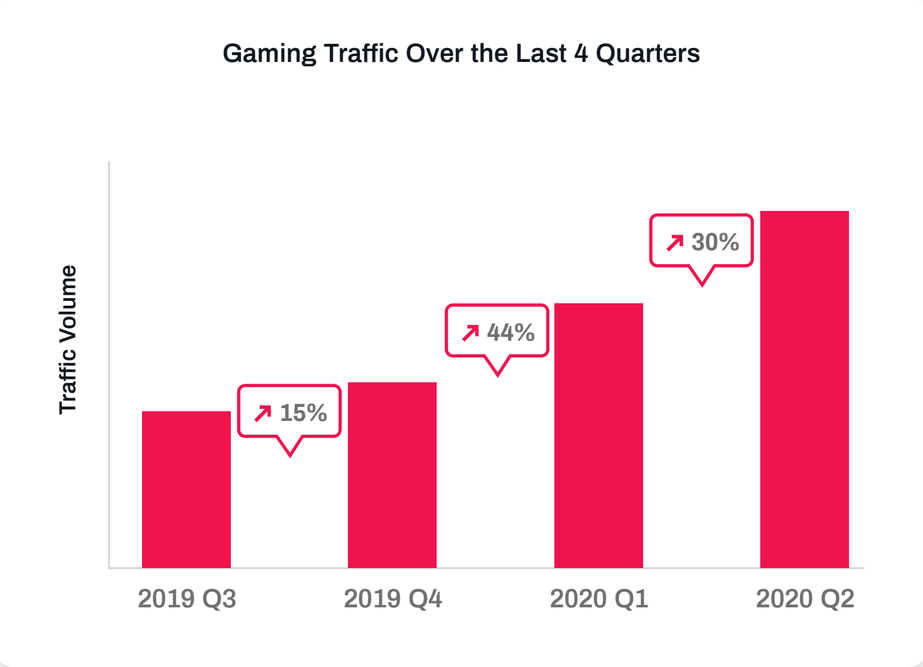
Q1 was dominated by automated attacks, as fraudsters leveraged tools to spin up attacks at speed as an immediate response to COVID-19. However, Q2 saw a shift to human-driven attacks, which accounted for 41% of gaming attacks. This returns the human attack mix to pre-lockdown levels, as 40% of attacks were human-driven at the end of 2019.

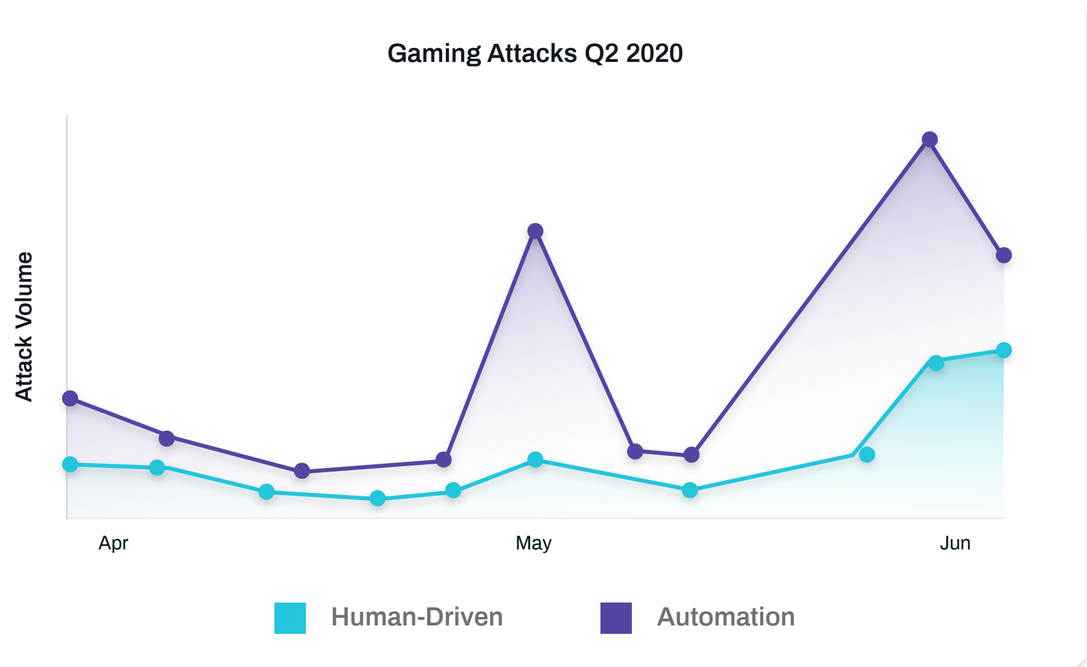


Gaming Traffic Explodes

Tracking the volume of gaming activity over the last four quarters demonstrates how big 2020 is proving to be for the industry. There have been major step changes in traffic volumes in Q1 and in Q2. High consumer activity makes this a top target for fraudsters.

Q2 2020 saw a steady increase in sweatshop activity, amid major spikes in automated attacks. Gaming companies were running high-profile promotions to attract customers, as competition hotted up during COVID-lockdowns. High traffic levels and additional pressure due to these promotional drives put systems to the test and required robust and highly scalable fraud prevention to fend off attacks successfully.



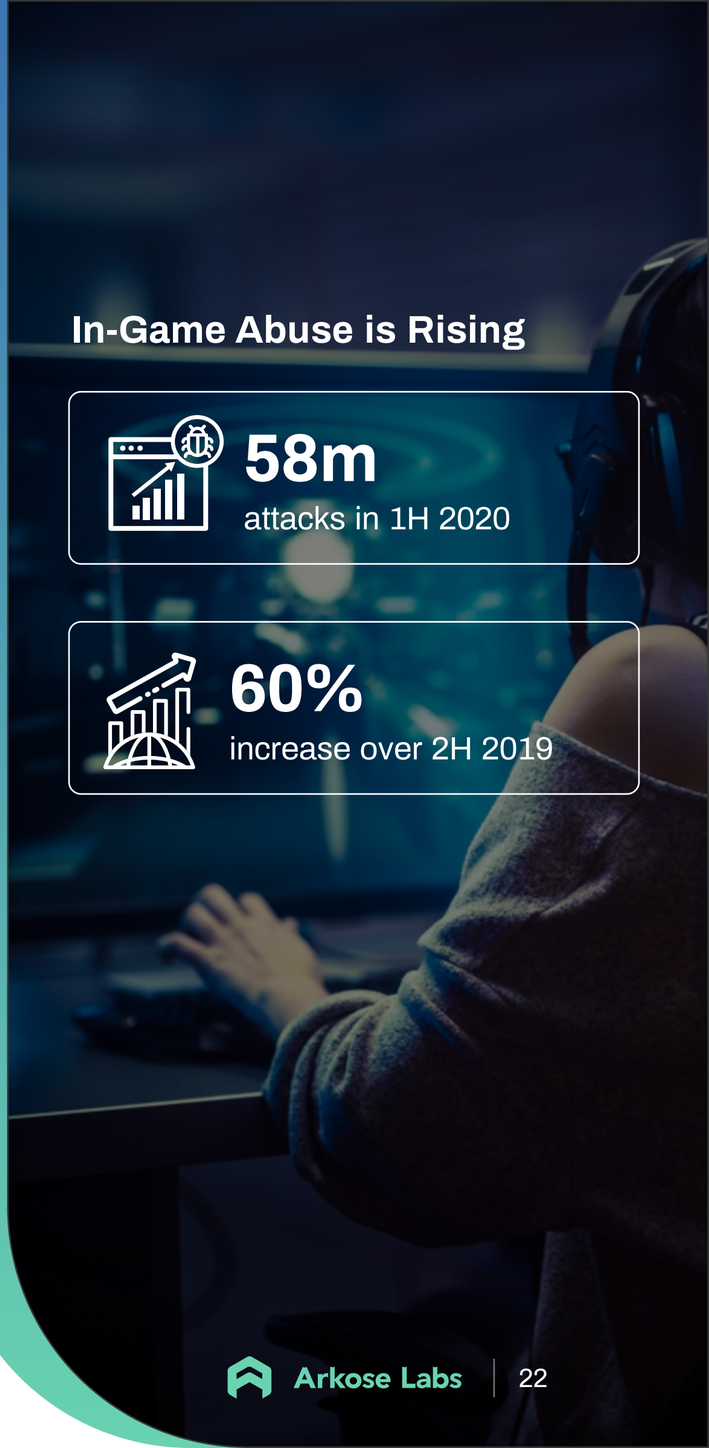


Spotlight on Real Money Trading

One type of abusive activity which is causing increasing damage to online gaming is real money trading. Click farms and bots are used to carry out abusive in-game activity, to farm gold, loot items or carry out repetitive actions that generate assets. These are sold on to other gamers through backchannels and illegitimate marketplaces. This pernicious activity can be a complex issue to solve. Banning malicious users downstream is a slow process and often proves a temporary fix. Therefore, gaming companies are often forced to roll back functionality, such as gifting and trading features, to the detriment of good users.

- Damages player sentiment
- Brand reputation suffers
- Harms user experience
- Takes away legitimate income selling assets
- Limits options for game designers

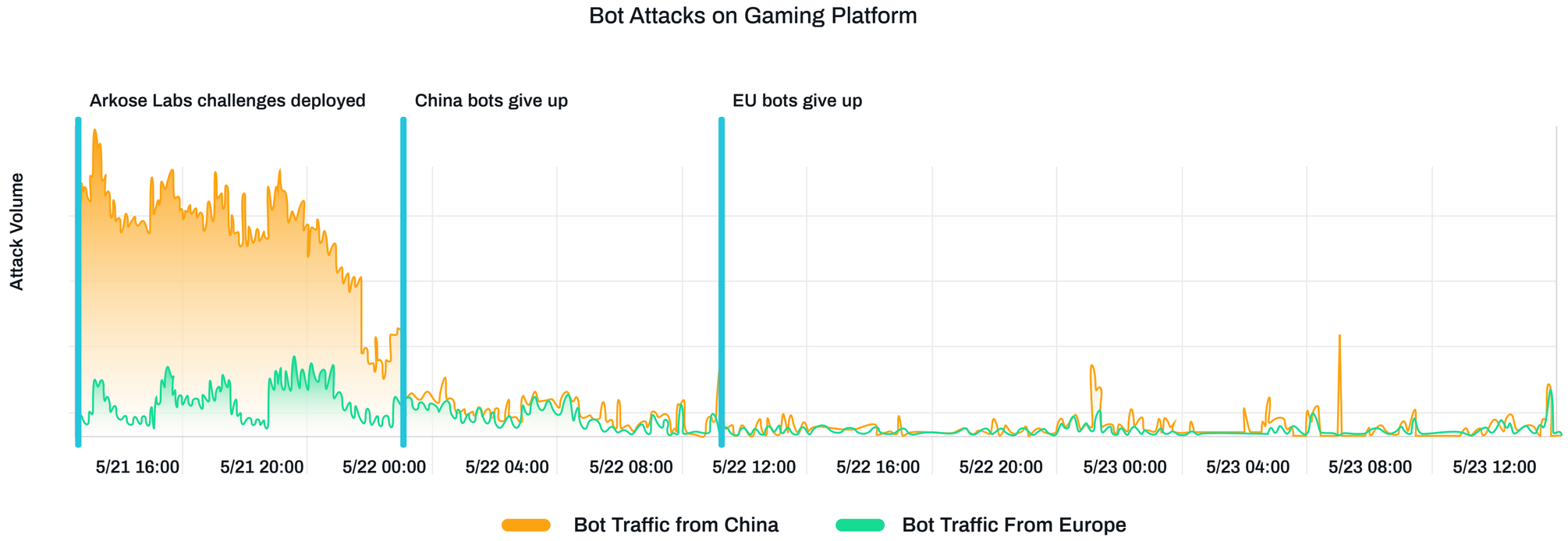
Arkose Labs is in a unique position to help address the issue of real money trading, as it can proactively monitor for malicious activity from logged in users deep within gaming platforms. Arkose Labs can spot suspicious activity and use in-band interactive challenges to remediate immediately, in a way that does not disrupt legitimate users. This way, gaming platforms can address issues in real time, rather than relying on downstream banning.



Gaming Case Study: Long-Term Deterrence Using Targeted Friction

A major online gaming platform, with millions of global users, was facing large-scale credential stuffing attacks originating from China and Europe. Online support pages for customers experiencing account login issues were being hammered by bots looking to hack into legitimate accounts.

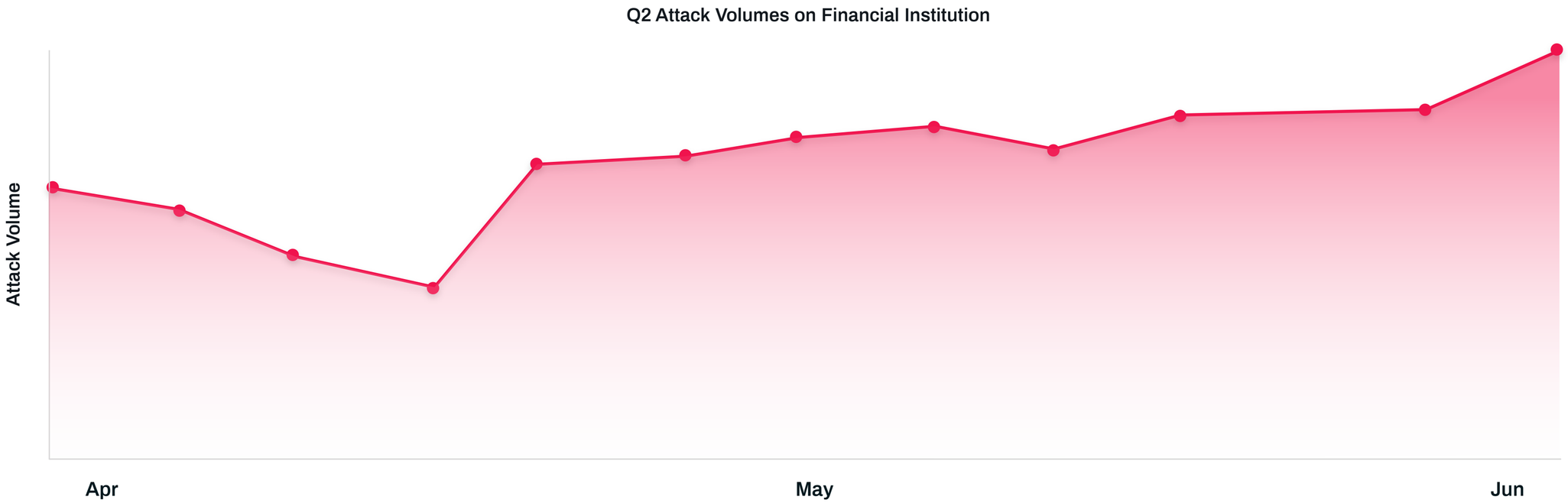
Within hours of Arkose Labs challenges being added to the flow, attacks from China dropped off, and within 24 hours the European bot attacks had also given up. There was no damage to legitimate traffic, showing the power of targeted friction in beating organized attacks.



Rising Attack Volumes on Finance and Fintech in Q2

Banks and fintech often pose the biggest challenge for fraudsters due to high investment levels in anti-fraud and security solutions. Therefore successful fraud attempts require more planning and orchestration than attacks on other segments.

Financial institutions on the Arkose Labs network saw attack levels rising notably in Q2, after an initial dip in April. These attacks were primarily driven by human sweatshop activity and targeted application fraud. 15.6% of attacks were on mobile transactions, as opposed to desktop, which is slightly below the cross-industry average for the mobile attack mix.



Human-Driven Attack Spike on the Technology Sector

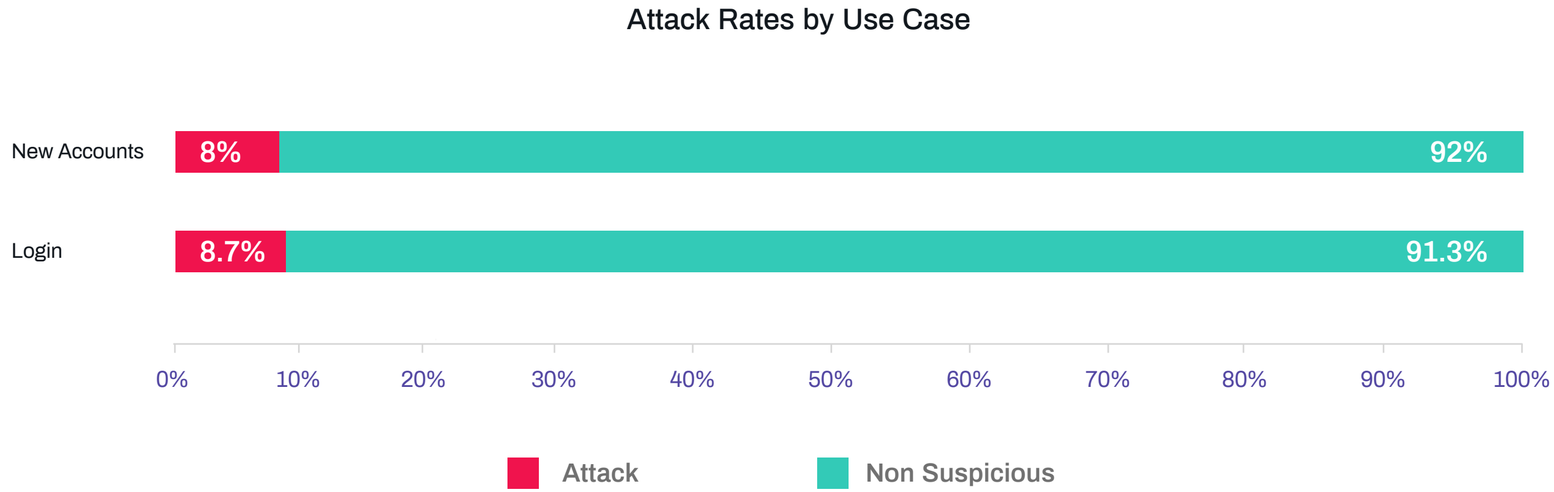
8.5%
attack rate

57% of attacks from sweatshops

27%
of attacks on mobile

The ability for users to communicate and collaborate digitally has never been more important. Alongside “lockdown”, “social distancing” and “isolation”, the word “zoom” has entered people’s day-to-day vocabulary - regardless of an individual’s preference on video calling platform.

As a result, the technology industry is witnessing an uptick in targeted attacks. There was a major swing towards human-driven attacks in Q2, with 57% of attacks now coming from sweatshops. Tech also had an elevated mobile attack mix, with 27% of attacks targeting mobile traffic.



Microsoft Outlook.com Tackles Fraud and Abuse Globally

Microsoft

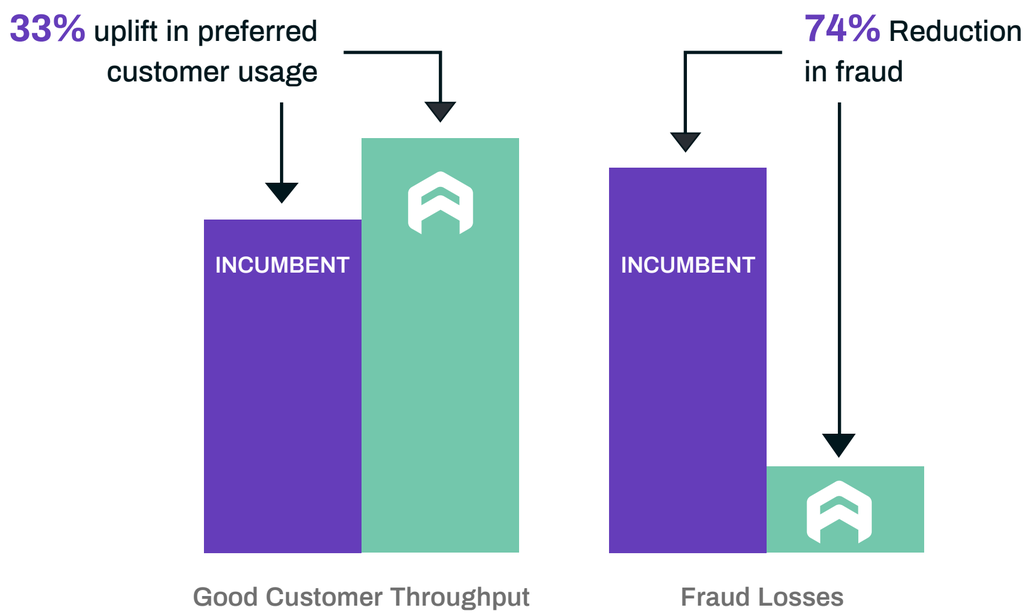
Outlook.com has hundreds of millions of active users, however, its popularity makes it a prime target for fraudsters looking to abuse new accounts to extort money or obtain sensitive information using malicious emails.

Business Problem

- Large-scale fake account registrations
- Email accounts used for malicious and fraudulent purposes
- Fraud mitigation disrupted good user experience

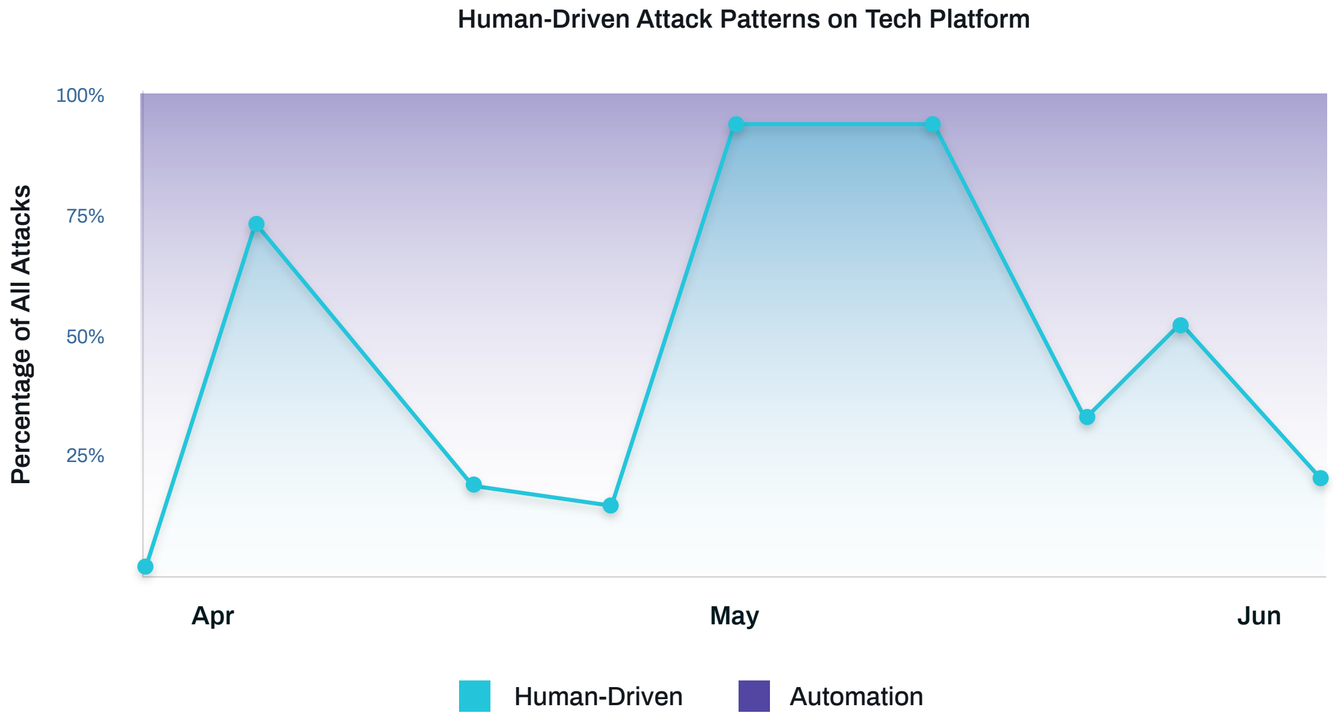
Solution

- Unified authentication for new users
- Innovative challenges stop bots and fraudsters
- Malicious emails detected and challenged downstream



Tech Case Study: Battling Human Fraud Operations

A global technology company was experiencing peaks in attacks, which the Arkose Labs team ascertained to be human-driven activity originating from a known solving solution. These operations use cheap human labor to bypass authentication challenges at scale. Whereas automated attacks can be addressed using simple interactive challenges, and regularly changing the nature of the challenge, the key to rooting out mass human-driven attacks is to increase the complexity of a challenge. These operations run on such small margins that any delay in their ability to complete challenges will deter click farm attacks long term. Using this strategy, Arkose Labs was able to effectively defend the tech platform from pernicious sweatshop-driven attacks.



Retail and Travel: A Tale of Two Industries

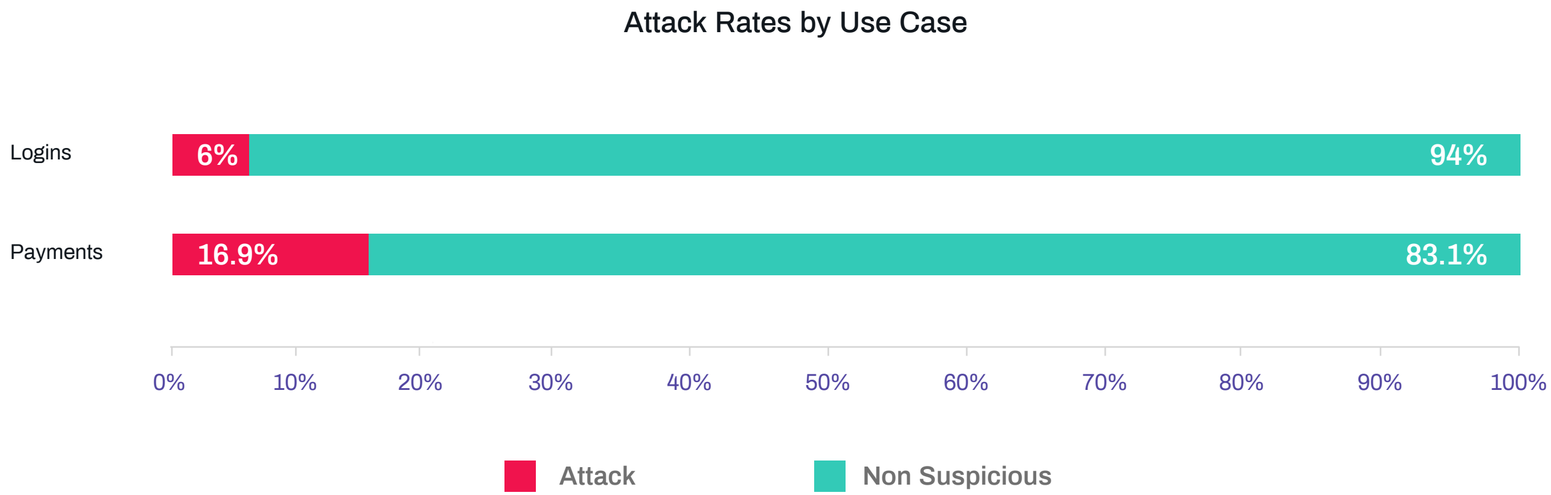
12.5%
attack rate

26% of attacks from sweatshops

13% of attacks on mobile

Retail has become a juicy target for fraudsters. Especially vulnerable are those businesses who have newly embraced digital commerce - mainly out of necessity due to lockdown measures. While new entrants to the ecommerce world will leverage payment processors to collect secure payments, there is still vulnerability at the account login stage.

One in five attacks originate from human sweatshops, however, these are almost all targeted ecommerce sites rather than travel - which has negligible human-driven attack levels due to the low traffic volumes in an industry devastated by COVID-19 travel restrictions.



Trend Spotting: Beyond Mitigation Focused Strategies

Gartner's Cool Vendor report this quarter flagged that in the current threat landscape, businesses need to go beyond mitigation-focused strategies that rely on threat scores and behavioral analysis. More robust fraud detection capabilities are required, in a way that still delivers great user experience. Arkose Labs' ability to combine risk assessments with targeted enforcement challenges in a user-friendly way, puts it in a unique position address this issue.

Arkose Labs was featured as a Gartner 2020 Cool Vendor in the report which highlights "interesting, new and innovative vendors, products and services" in the IAM and fraud space.

Gartner
COOL VENDOR 2020™

Cool Vendors in IAM and Fraud Detection

Highlights from the report:

"The balance between detecting and mitigating fraud and creating low-friction and seamless UX has never been as important."

The limitations of mitigation-focused strategies in defeating fraud and automated abuse.

Traditional CAPTCHAs are being beaten by automation.

Download the full report at arkoselabs.com/gartner

Conclusion: The Road Ahead in 2020

In recent years, the driving factor behind rising fraud attacks was the prevalence of high-profile data breaches on major companies. This spurs fraud on by providing fresh swathes of user data that are leveraged in downstream fraud attacks.

In 2020, however, these publicity-grabbing data breaches have been conspicuous in their absence. The cybersecurity headlines have been dominated by COVID-19 related scams, for example phishing attacks or attempts to hijack government relief checks in the United States; or security concerns around social media, which as the primary loudspeaker for political and social discourse is being targeted by bots and account hacking.

Alongside these issues is a steady rise in the intensity of fraud attacks hitting digital businesses today. The volume of attacks on the Arkose Labs network has doubled since the end of last year, alongside the acceleration of digital traffic due to the COVID-19 pandemic. More people have become comfortable transacting online, and remote communication and digital education platforms will continue to boom.

This change in digital habits is a double-edged sword for businesses; it brings more people into digital channels, but also provides greater opportunities for fraudsters to attack and blend in with normal online traffic. These are irrevocable trends, and businesses must be prepared to handle the onslaught of fraud that comes with increased digital adoption. Those that do will gain a clear competitive edge going forward.

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.

About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319

Offices

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

Brisbane
315 Brunswick St, Brisbane, Queensland AU