Arkose Labs

Fraud & Abuse Report | Q4 2020

Data-Driven Analysis of 2020 Fraud Trends

Introduction

The explosion in digital activity in 2020 is redefining many businesses' world view. Digital offerings are suddenly serving a far wider customer base than they were designed for, upending entire business models. Unprecedented digital activity is coinciding with a socio-economic landscape that has pushed fraud inventive levels sky high. Even mature economies have experienced staggering drops in GDP since COVID-19. While advanced threat actors are devising innovative new attack methodologies, there is also a new wave of entry-level fraudsters. Easy access to turn-key tools and swathes of stolen data helps fuel the increased volume and intensity of attacks.

The Arkose Labs network saw its highest ever levels of bot attacks during Q3 2020. Credential stuffing was a big driver of that attack traffic, with 770 million automated login attempts detected. Europe emerged as an epicenter for fraud; around half the attacks detected on the network now come from Europe, with Russia alone accounting for 483 million attacks. As the world remains more digital, and the economic turmoil brought on by the pandemic continues, businesses need long-term strategies to defend against high velocity fraud and abuse, while successfully serving their growing digital customer base.

Kevin Gosschalk
Founder and CEO

As the world is more digital and economic turmoil continues, heightened attack levels are here to stay. Businesses need long-term strategies to defend against high velocity fraud and abuse.

Q4 Fraud & Abuse Report At a Glance

2020 in Numbers (January to September)

2.4 Billion
attacks detected

18%
sweatshop vs automated

16%
mobile vs desktop attacks

Q3 Global Attack Trends

1.3 Billion
attacks detected

770 Million
credential stuffing

biggest automated attack quarter on record

64%
of attacks on logins

85%
desktop attacks

15%
mobile attacks

Q3 Regional Attack Trends

Europe
biggest attacking region

49%
of attacks from Europe

493 Million
attacks from Russia

Key Trends And Predictions

Holiday Season

The rise in digital traffic for most of this year means that businesses have been dealing with holiday season levels of traffic since March. Traffic levels and fraud attacks could become even more pronounced during this holiday season, which could be the biggest ever for digital commerce.

State of The Digital Economy

The COVID-19 economy has created clear winners and losers. E-commerce sites, gaming platforms and workplace collaboration tools have seen huge rises in popularity. These have, naturally, been industries that have attracted fraud attacks. Travel and booking are hurting in a world where many are sheltering in place, but even they are still seeing some levels of fraud activity, particularly with ATO attacks and fraudsters seek to monetize unused rewards points.

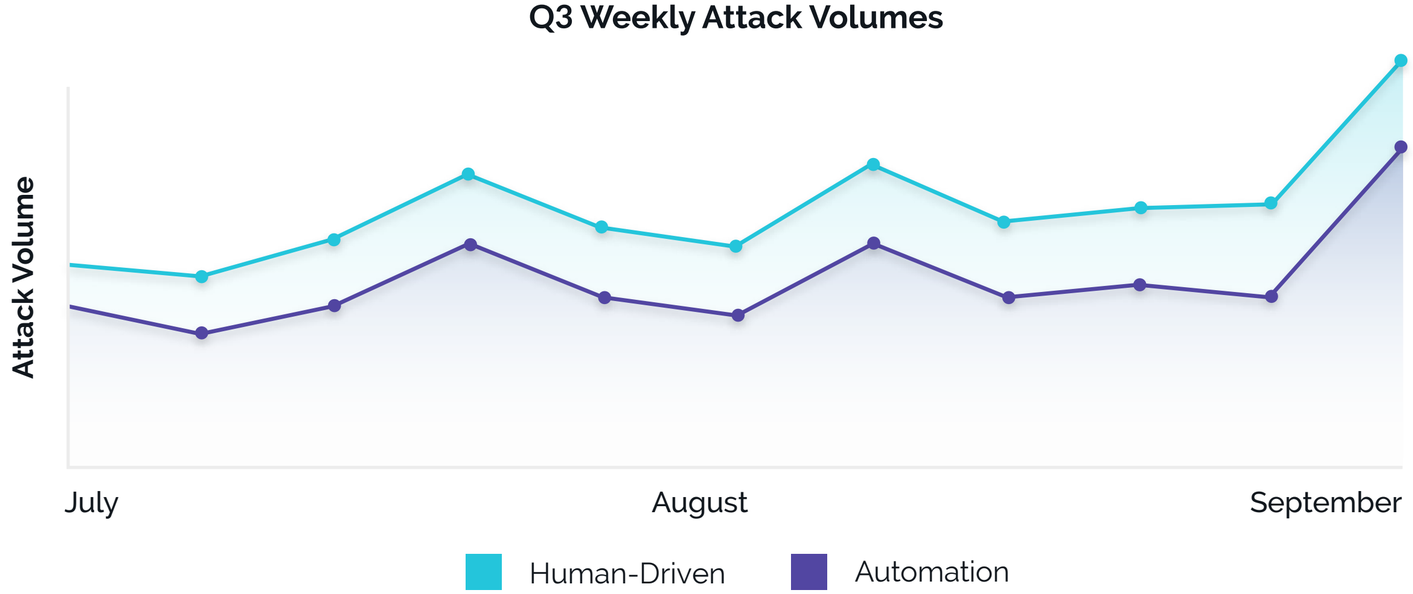
Fraud Monetization

Fraudsters are using ATO attacks not only for the information itself held in accounts, but also to power other downstream fraud, such as reselling personal data to third-party sites, laundering money or launching phishing scams. Gift card fraud is also becoming more popular (see page 18) since it can be extremely difficult to track and trace.

Q3 Weekly Attack Trends

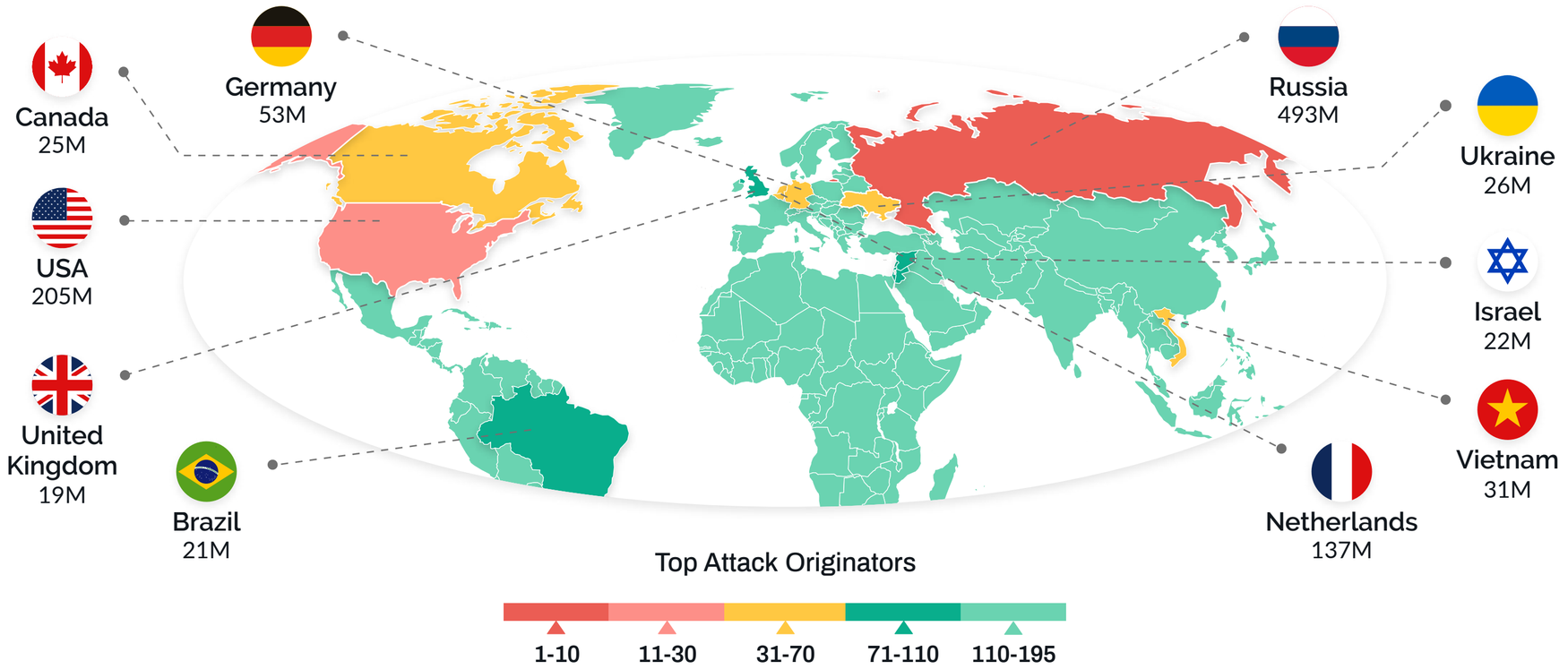
Bots were a big driver of fraud attacks during Q3, and the proportion of attacks coming from sweatshops was down compared to the previous quarter. 2020 has witnessed an overall increase in attack volume, which started with COVID-19 lockdowns in the spring and still show no signs of slowing down; in fact they were still rising as Q3 ended. A permanent increase in bot attacks may be the "new normal."

Automated attacks can scale up quicker than sweatshop attacks, greatly surpassing human attacks in sheer volume, if not sophistication. This is why bots were the main driver of attacks in Q3, with human-driven fraud supplementing them in more targeted attacks that require human intervention.



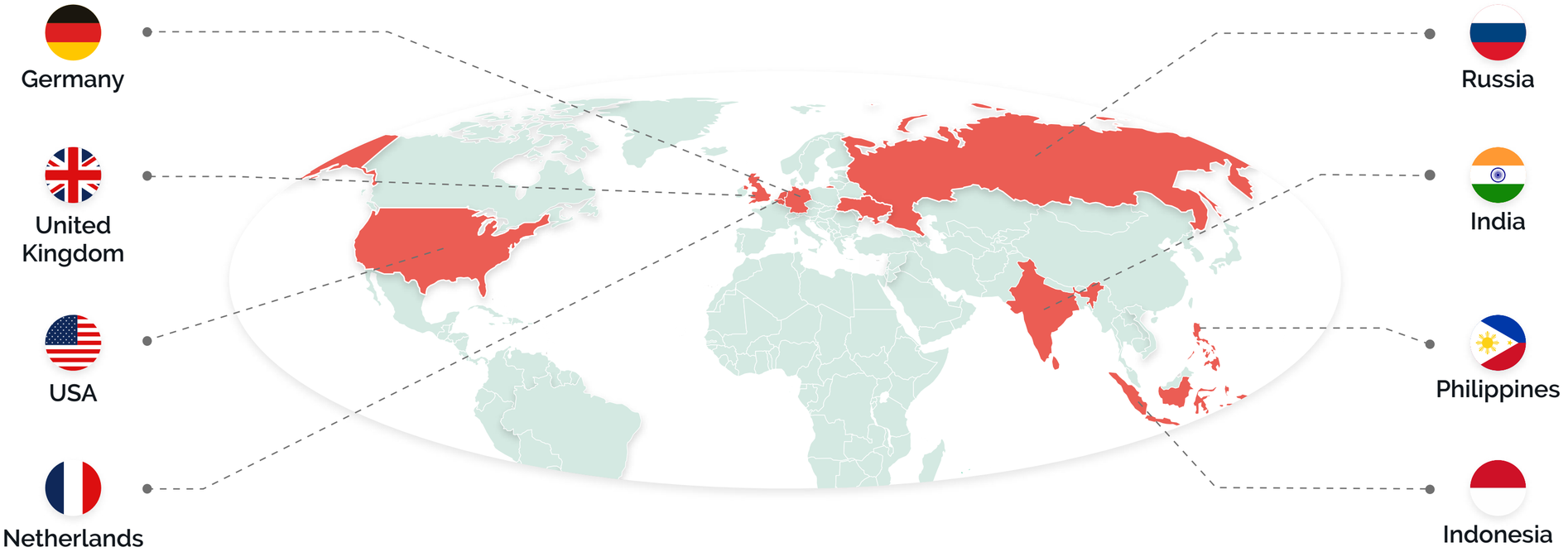
Top Attacking Countries in Q3 2020

Continuing a trend seen in Q2, the top countries of origin for fraud attacks are shifting towards well-established economies. This is a bit different from the traditional fraud hubs, which are typically seen in developing economies. This time last year, the Philippines topped the charts of attack origination, whereas it does not even feature in the top ten in Q3 2020. A likely driver of this is financial hardship; as Covid-related economic turmoil continues to roil most of the world, people are more willing to turn to fraud to make ends meet. This also points to the interconnectedness and efficiency of the global fraud ecosystem. Fraudsters can quickly mobilize to take advantage of changing socio-economic circumstances to recruit new participants and scale up attacks.



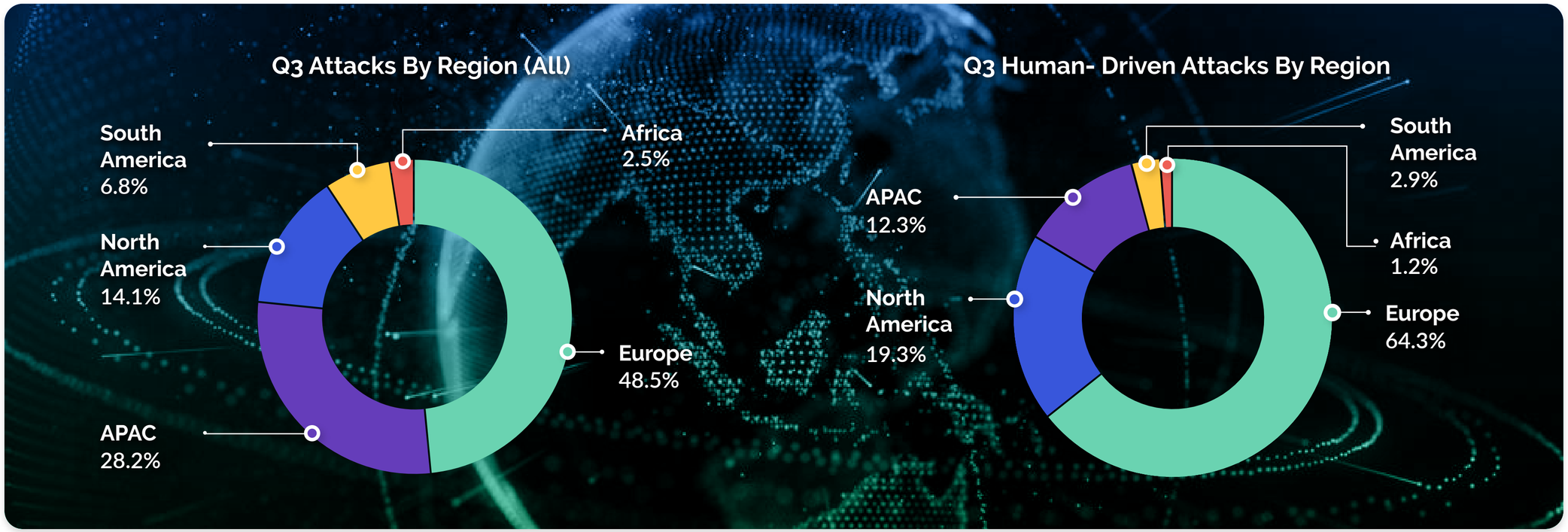
Sweatshops: Top 10 Attacking Countries

A vital component in the fraud ecosystem are organized sweatshops of low-skilled and low-paid workers, which help carry out attacks at scale and circumvent defenses designed to root out bot attacks. Due to the economics involved, these attacks have typically come from countries with a low cost of living. In Q3, however, there was a surprising amount of sweatshop activity coming from developed economies, such as the U.S., Great Britain and the Netherlands, as well as more traditional sweatshop hubs, Such as the Philippines and Thailand. Again, this is likely due to COVID-19 lockdowns severely impacting millions of jobs, causing individuals to search for new streams of revenue online. This is a trend that will likely continue into coming months, as face-to-face interactions remain restricted due to the pandemic.



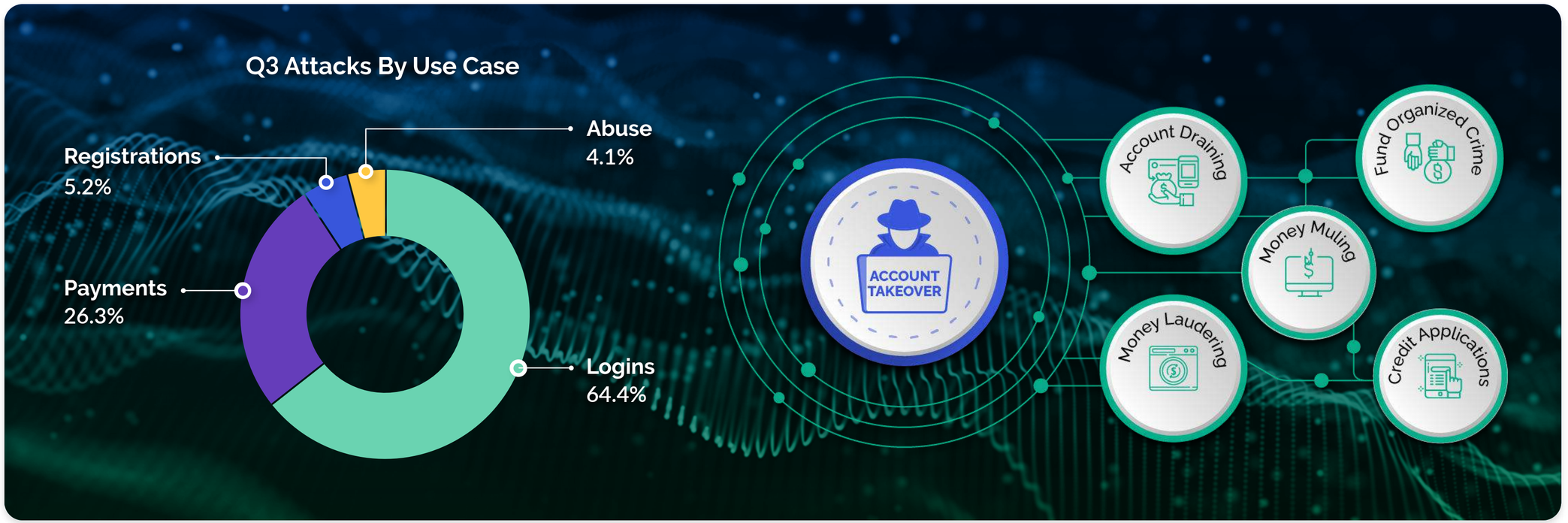
Regional Trends: Surge in Attacks From Europe

Nearly half of all attacks in Q3 2020 emanated from Europe. Interestingly, many European countries are among those whose GDP has shrunk the most since the COVID-19 pandemic began. This includes the United Kingdom, France, Italy and Germany, all of which have suffered a 10% or more reduction in GDP during the pandemic. The surge in attacks from nations suffering the biggest dips in economic output highlights the economic drivers that spur on fraud attacks. Looking at the data of human-driven fraud attacks, a massive 64% of attacks originate from Europe, with over 10 million attacks from Russia, and 7 million attacks from the United Kingdom.



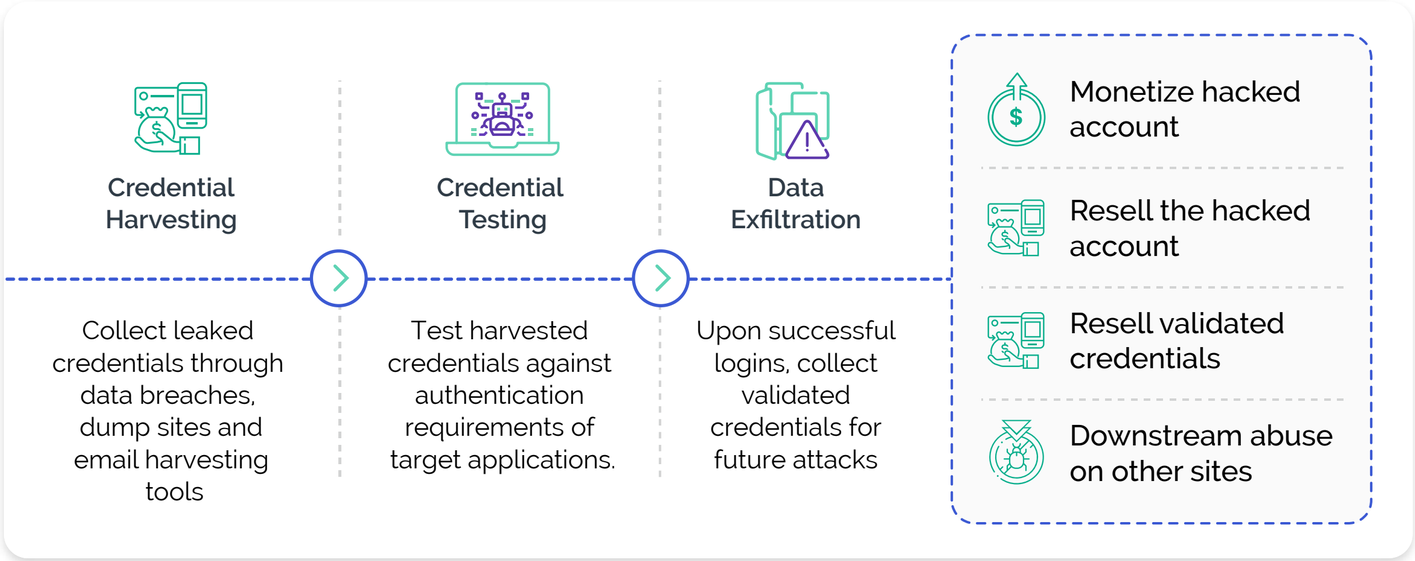
Account Logins the Most Attacked Touchpoint

Logins are the most attacked customer touchpoint, due to a mix of automated credential stuffing and more targeted human-driven attacks. Account takeover attacks can power a lot of downstream fraud. Compromised accounts are used to send spam and phishing messages; steal personal data; drain funds; or channel the proceeds of organized crime, such as drugs, human trafficking, and terrorism. 7% of attacks came under "abuse", which encompasses scraping, in-game bots within gaming platforms, and fake reviews on marketplaces and peer-to-peer sites. This sort of malicious activity can be a major headache for certain sub-industries.



Spotlight on Credential Stuffing

In October 2020 the FBI issued a warning around the rise of this attack vector, reporting that 41% of cyber attacks on the financial sector are from credential stuffing attacks. The Arkose Labs network detected and stopped some 770 million automated credential stuffing attacks in Q3 2020. Credential stuffing is on the rise due to the easy availability of usernames, email addresses and passwords from years of data breaches, and easy access to automated tools to carry out these attacks at scale. It only takes a minimal amount of effort and money for fraudsters to launch credential stuffing attacks, testing thousands or even millions of combinations in minutes.



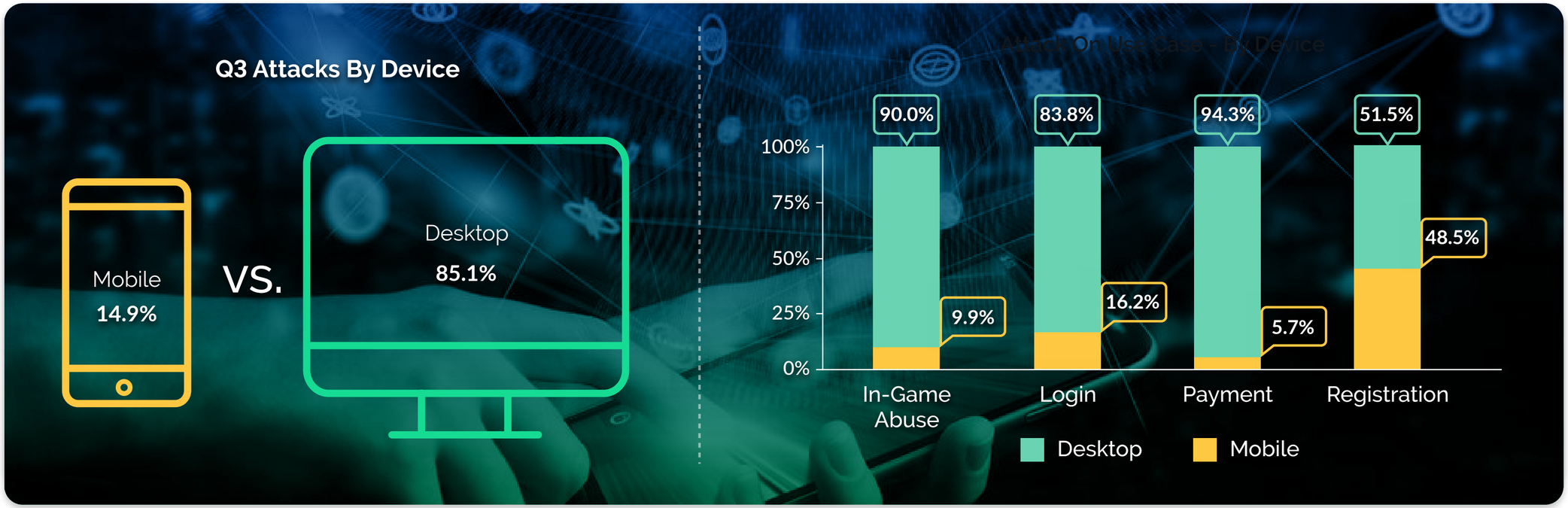
770M

automated credential stuffing attacks in Q3 2020.

Mobile Attack Trends

There was a slight dip in the mobile attack rate between Q2 and Q3, falling from 21% of all attacks to 15%. This can be attributed to the dominance of bot attacks this quarter, which are more likely to be driven from computers rather than mobile devices.

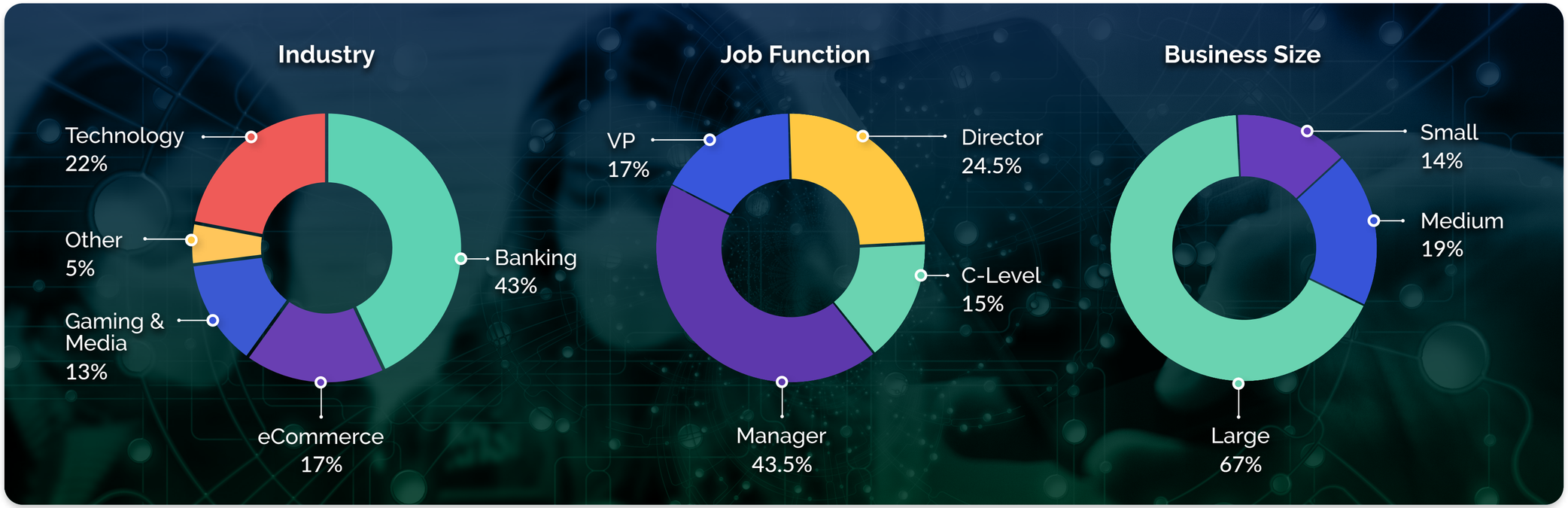
When examining the attacks by different use cases, the mobile attack rate fluctuates greatly. For new account registrations, nearly half of attacks are carried out on the mobile channel. This is probably due to the ease with which new accounts can be opened on a mobile device in some industries, such as social media, dating and streaming. In comparison, only 6% of payment fraud was conducted via a mobile device.



COVID-19 Fraud Trends Survey

2020 has been a year like no other, as COVID-19 has wreaked havoc across the globe. Businesses have seen disruption on an unprecedented scale with mass lockdowns worldwide, and millions of people working from home.

Arkose Labs assembled 80 fraud and security professionals to get insights into 2020 fraud patterns in the wake of the COVID-19 pandemic. Industry experts came largely from large enterprises, from companies including Netflix, Capital One, Zendesk, Amazon, Wells Fargo, Dropbox, Microsoft, PayPal and Uber.



COVID-19 Survey: Reports From the Frontline

The 2020 Fraud Survey highlighted attack vectors that accelerated during the COVID-19 pandemic, and are causing greater concern for businesses in 2020.

Credential Stuffing

Experts across all industries reported a rise in credential stuffing attacks as fraudsters seek to compromise a bevy of new accounts created during the pandemic.

Social Engineering

With more people than ever before living and working in semi-isolation, it is easier for fraudsters to successfully launch scams, such as phishing attacks. They especially target new digital users who have come online during the pandemic.

Identity Theft

Children have become a new target for identity theft, as they have spent most of the year logged onto digital classrooms, social media, and gaming networks. They are often unsupervised and are seen as easy prey by fraudsters.

COVID-19 Scams

Fraudsters pretending to be official agencies have engaged in a wide range of scams designed to play on consumer identity, especially around issues such as stimulus checks and small business loans.

Friendly Fraud

There has been a significant rise in chargebacks and friendly fraud, especially as pandemic-related financial hardships blur the line of what is acceptable for many.

First Party Fraud

Financial institutions are a prime target for first party fraud, where individuals or small businesses take out a loan with no intention of ever repaying it.

COVID-19 Silver Linings

However, it wasn't all doom and gloom: survey respondents also reported some positives coming out of COVID-19. The main positive takeaway was that companies had to pivot quickly and learn to operate effectively during a highly unexpected event. This should better prepare businesses in the future for other "black swan" events.

Collaboration

The pandemic has brought about a more collaborative approach to fighting fraud. Competitors have become allies, as companies share information on fraud trends and present a united front against fraud.

Stress Test Systems

While an explosion in digital traffic amid COVID-19 took attack volumes to unprecedented levels, it also enabled fraud teams to stress test their systems, identifying weak spots and strengthening strategies for the future.

Remote Working

Many fraud teams reported having a successful switch to a remote working model. However, it has also caused data protection headaches and increased the risk of information being stuck in silos between teams.

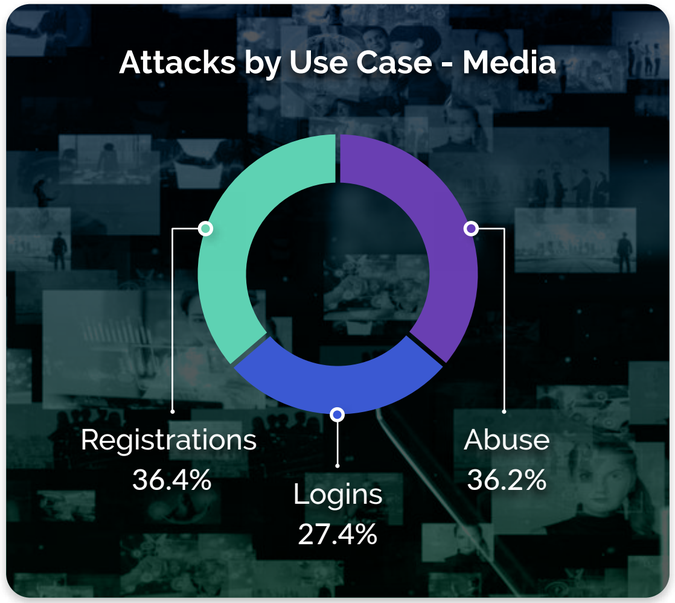
Media Industry Sees Variance in Attack Points

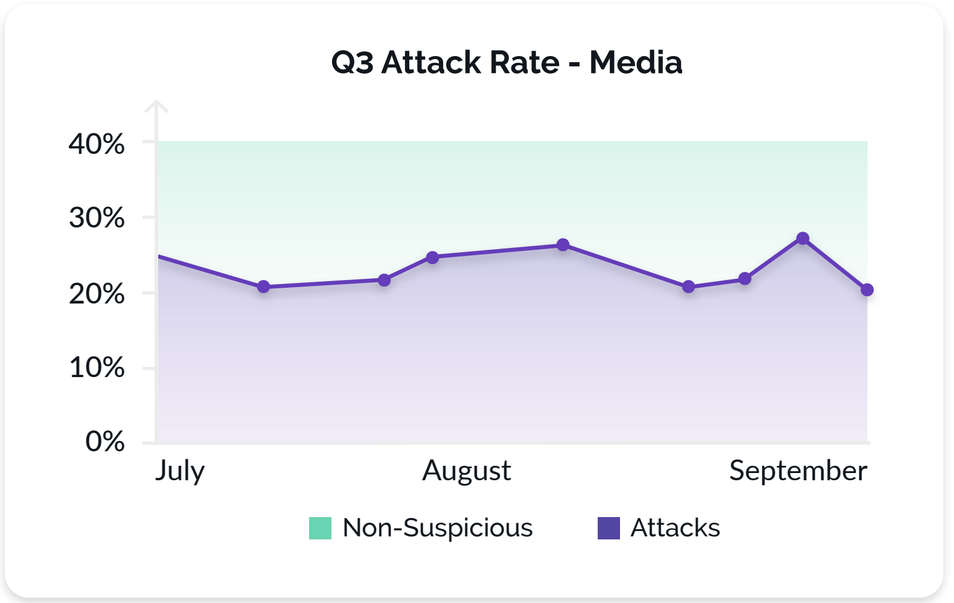
7%
attack rate

23% of attacks from sweatshops

37%
mobile vs desktop

Media companies on the Arkose Labs network span social media, dating apps, and digital streaming services. As people have been confined to their homes more than normal since COVID-19, digital entertainment platforms have seen a surge in users. Streaming companies on the network were primarily targeted with automated credential stuffing attacks in Q3 2020. On the other hand, social media platforms were targeted with a far wider range of fraud and abuse. This includes automated scraping, which seeks to steal and resell personal information; account takeover attacks; plus fake account registrations. Social media also sees a higher proportion of sweatshop attacks compared to the bot attacks targeting the rest of the sector.





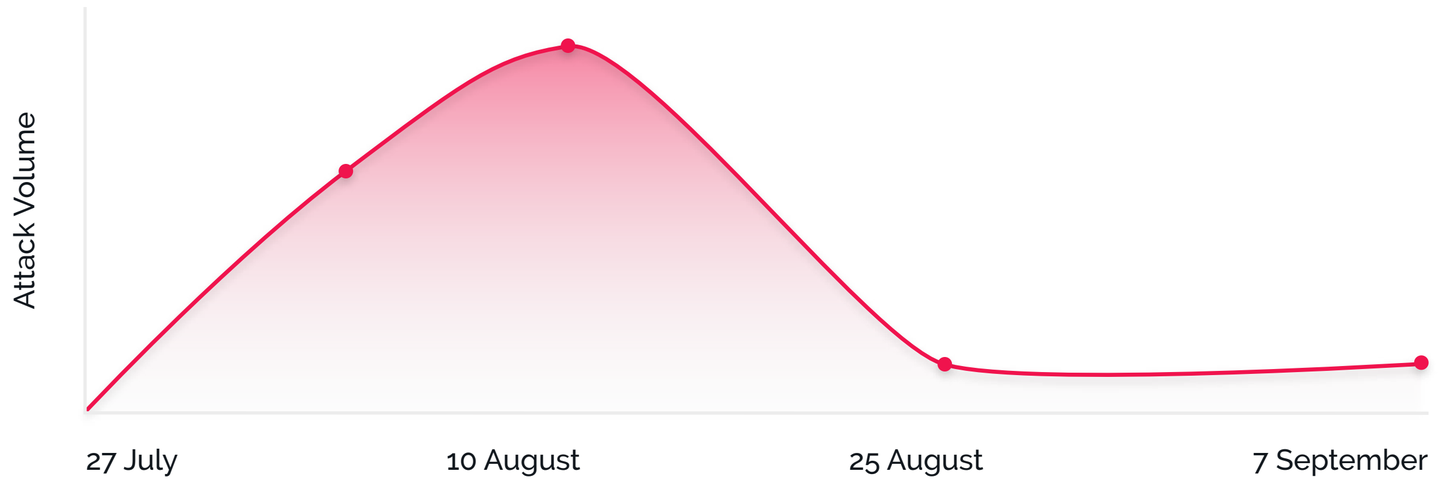
Case Study: Streaming Company Sees Fast Results Since Deployment

A well-known digital streaming company with millions of users deployed the Arkose Labs platform, to protect logins and new account registrations. The company saw results almost immediately, as the Arkose Labs platform detected and remediated attacks in real time; challenging fraudulent traffic whilst still preserving good user throughput, which was the company's chief objective. Immediately after deploying the solution, it was detecting new attacks - which saw a quick drop off as challenges were deployed and deters future attempts.

95.4%
of users pass unchallenged

99.4%
Challenge completion rate for good users

Quick drop-off of attacks for long-term deterrence



Retail and Travel: Changing Fortunes

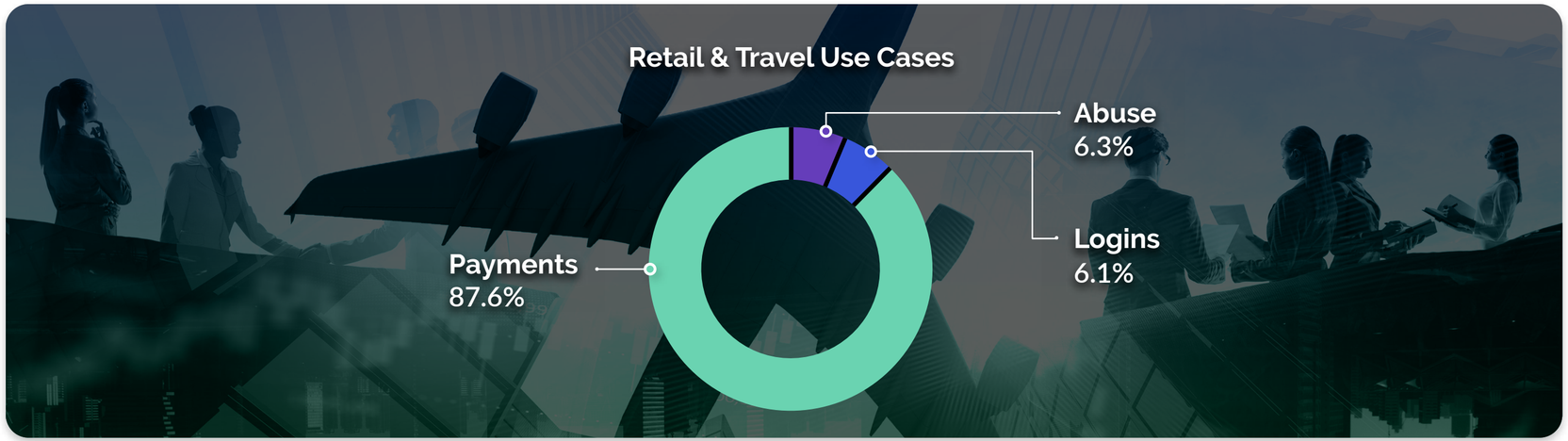
7.3%
attack rate

38% of attacks from sweatshops

48%
mobile vs desktop

Nearly all attacks on retailers on the Arkose Labs network were at the payments stage - which is where retailers focus most of their fraud defenses. Ecommerce sites were always a big target for fraudsters, but are under far more pressure in 2020. Rising fraud levels come alongside the increase in traffic amid lockdowns and the addition of "digital debutantes" who adopted online shopping during the pandemic.

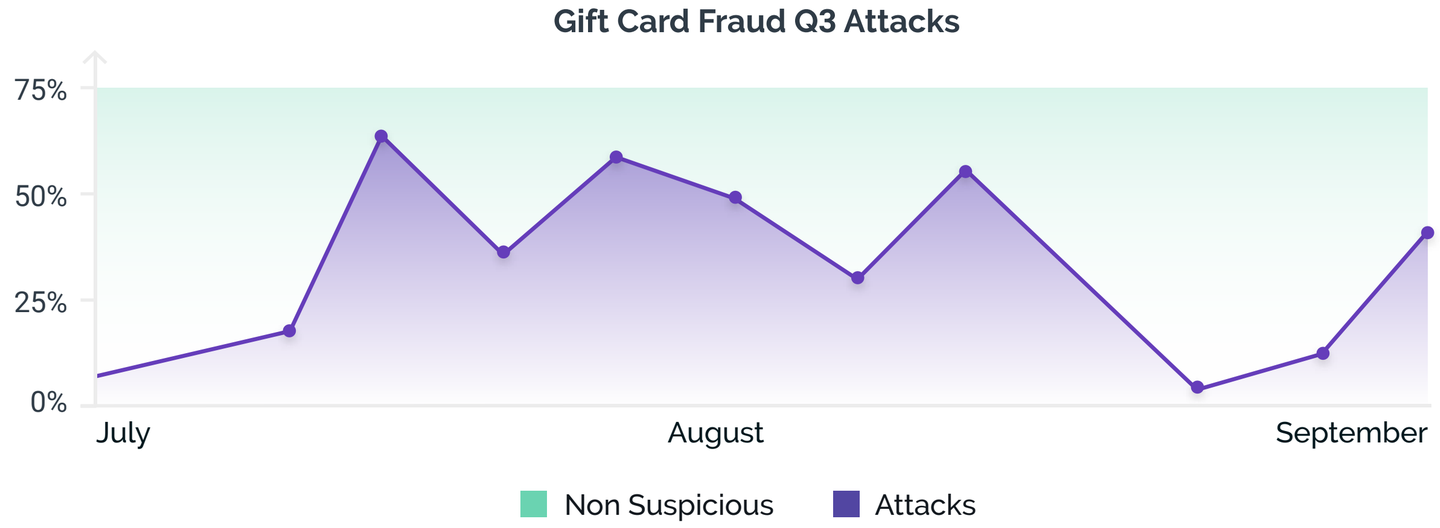
A subset of this sector is travel, which has a very different outlook. The travel industry is being hit hard by the pandemic. It is seeing very low attack levels due to the drop-off in legitimate transactions. 50% of malicious activity detected in the travel industry in Q3 2020 fell into the "abuse" category - mostly information scraping and fake reviews. The other 50% are fake new account registrations, as fraudsters use these sites to test stolen credentials. 97% of attacks are automated; with bad actors unwilling to expend time or energy attacking this sector at the moment.



Spotlight on Gift Card Fraud

The gift card industry is a frequent target of fraud attacks. Fraudsters particularly like abusing gift cards and prepaid cards because they offer direct monetization and can be extremely hard to trace, making it easier to hide their tracks. Fraudsters routinely employ both sweatshops and bots to check card balances and redeem stolen gift cards.

There has been a recent rise in abuse in this area due to prepaid cards being used as a vehicle for government stimulus money for those who did not have bank accounts on file with the IRS. A common scam involved fraudsters making phone calls telling consumers they could take the money off the card for them and send a check, and asking for the card details.



The Many Faces of Gift Card Fraud

Gift card fraud is appealing to criminals because of the anonymity involved, it is essentially like stealing cash. Here are some common ways gift cards are abused.

Hacking linked bank accounts

If a consumer utilizes an auto-load feature with a gift card, fraudsters can hack into the account and quickly drain it of funds. It's easy for the fraudsters to get away with this since the money is going to a gift card, as opposed to another bank account.

Redeeming loyalty points

Fraudsters often hack into accounts to redeem loyalty points, such as those associated with a credit card or travel account. Since those are often linked to the user's bank account or address, redeeming the points as a gift card is a quick and easy way for fraudsters to cash out the points balance.

Stealing numbers

In this type of fraud, a bad actor will steal a stack of gift cards from a store, write down all the numbers, then return them to the store shelf. The fraudster will then continually check those numbers to see if and when they have been activated by a legitimate activation, then quickly drain the funds.

Spotlight on Holiday Shopping

Normally, retailers expect the holiday shopping season to be much busier than the rest of the year. But with COVID-19 driving people online in record numbers, almost every day has become Black Friday. In some ways this has helped retailers better prepare for the holiday season onslaught of traffic (and fraud). However, there are still likely to be some unique trends to the holiday season to look out for.

The End of Black Friday?

The holiday shopping season has become synonymous with lines out the door of physical retail locations and people trampling one another to grab a plasma TV. But with consumers shopping digitally in droves, and retailers having Black Friday- esque deal events throughout the year, we could see the beginning of the end of this retail staple. All Black Friday deals that do happen, however, are likely to be kept online to avoid people gathering in stores.

No More Holiday Sales Bump

The holiday season is when the bulk of sales happen for retailers, for example in Q4 2019, the retail sector saw double the amount of traffic compared to the previous quarter on the Arkose Labs network. This may not be the case this year, as traffic levels have been at holiday levels since March for many ecommerce businesses.

More Human-Driven Attacks

The 2019 holiday season saw a marked shift from automated attacks to human sweatshop attacks. Therefore, it is interesting that Q3 has been such a strong quarter for automated attacks - this could very well swing back towards more targeted attacks again in Q4 2020 In the holiday shopping season, fraudsters employ low cost attackers to commit attacks that require human nuance and intelligence.

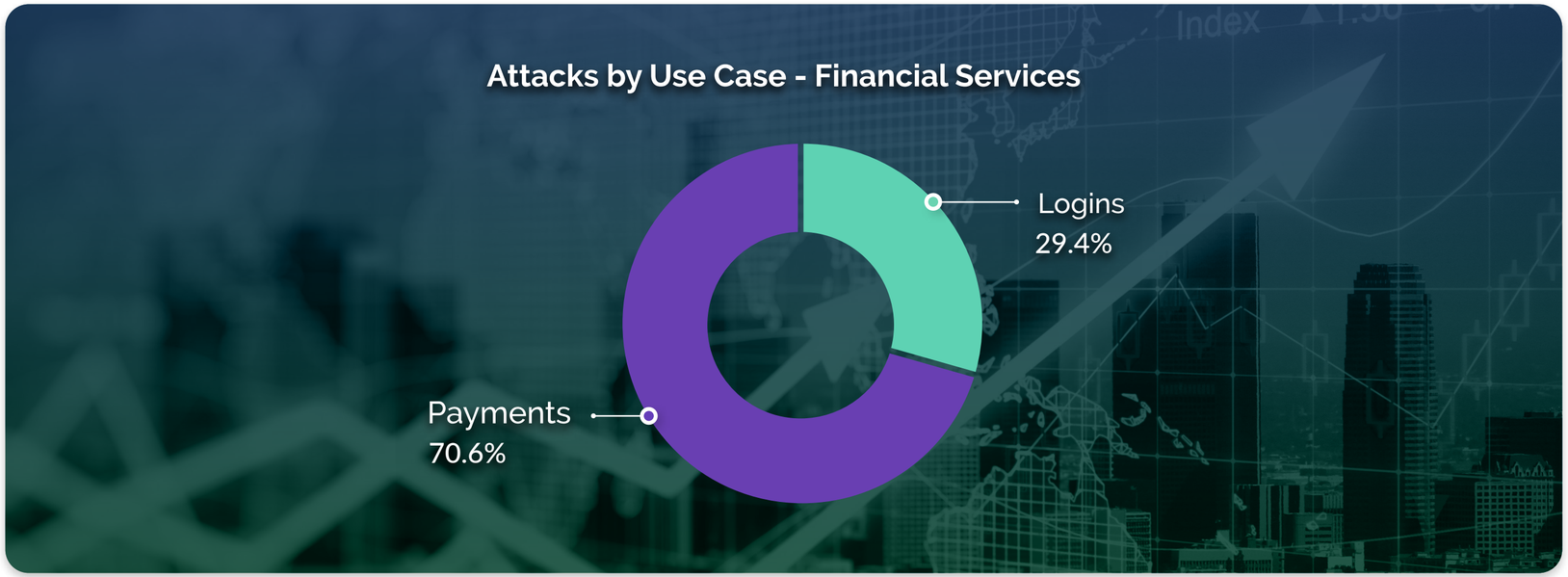
Fraud for Financial Services in Fintech in Q3 2020

Financial services are seeing the economic turmoil of 2020 spur on financial fraud. For example, in a desperate bid to access credit, consumers in financial straits will misrepresent income levels.

The majority of the attacks on the Arkose Labs network for this sector was at the payment stage. As more people embraced digital payments during the pandemic, fraudsters have targeted these touchpoints. Consumers expect these payments to be frictionless and instantaneous, and fraudsters in turn seek to hijack digital payments in real-time before any party is aware. 22% of attacks came from the mobile channel versus desktop, which is an increase in mobile attacks since the previous quarter.

70%
attacks on payments

22%
mobile vs desktop



Gaming Q3 Attack Trends

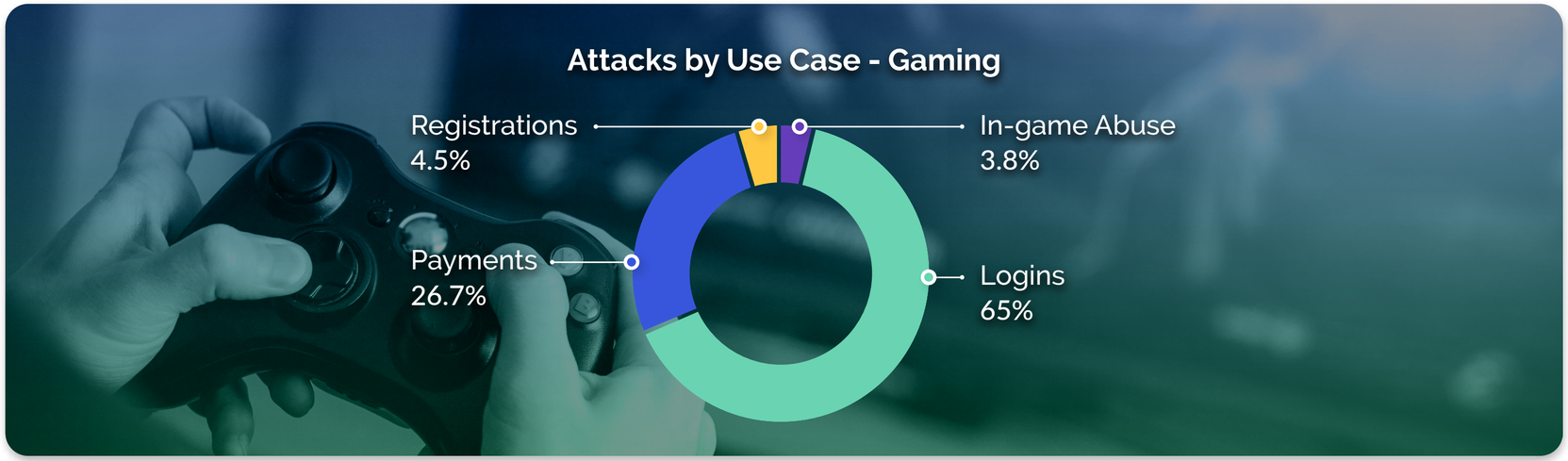
39%
attack rate

95% of attacks from bots

14.5%
mobile vs desktop

Gaming is one of the industries that has been most impacted by the pandemic. As lockdown measures quarantined people in their homes for months on end, many turned to online gaming platforms for leisure and to keep children entertained. Fraudsters, in turn, flocked to these platforms, attempting to blend in with the higher rates of traffic, leading to a 39% attack rate for the industry overall, which is a major increase since the previous quarter.

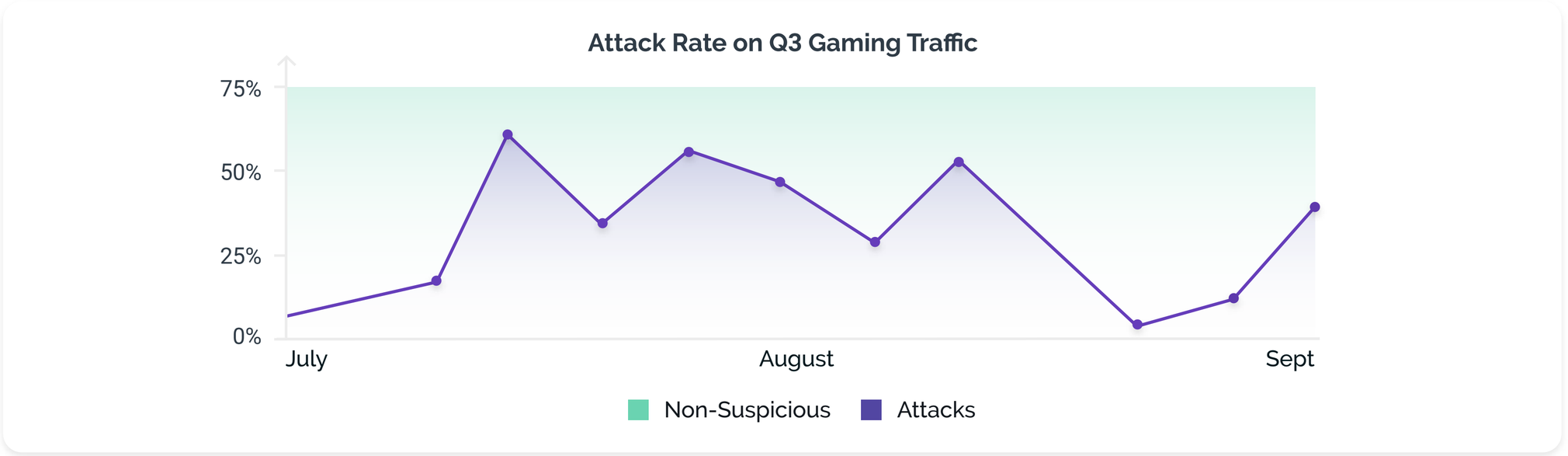
Fraudsters largely deployed bots to attacks on gaming platforms in Q3 2020, with 95% of attacks being automated. 65% of these attacks were on the login, with bad actors looking to takeover legitimate accounts to resell or perform downstream abuse. In-game abuse includes farming assets and gold, committing auction house abuse, and sending spam and phishing messages to other users.



Gaming: Extreme Volatility in Attack Rates

The biggest surprise in attack patterns in gaming was the sheer volatility of attack rates from one week to the next. Attacks ranged from more than 70% of all traffic in some instances down to very low levels in one September week. Bots are the preferred method used to carry out attacks at scale.

The intensity of attacks since COVID-19 is due to new entrants coming into the world of fraud - those who aren't necessarily professionals, but rather those committing fraud "casually" during the pandemic. Many keep doing it because the pay is good, and they had no other options at the time. By increasing the irritation factor in fraud defenses and making their work more difficult and time-consuming, businesses can effectively start rooting out this fraudster profile and compel them to abandon their attacks.



Gaming Case Study: Thwarting Credential Stuffing

A major online gaming platform was experiencing account takeover attacks. Attacks dropped off immediately after deploying Arkose Labs, however, fraudsters quickly pivoted and tried to adapt their attacks. This led to subsequent spikes in attack volume which were detected by the Arkose Labs platform.

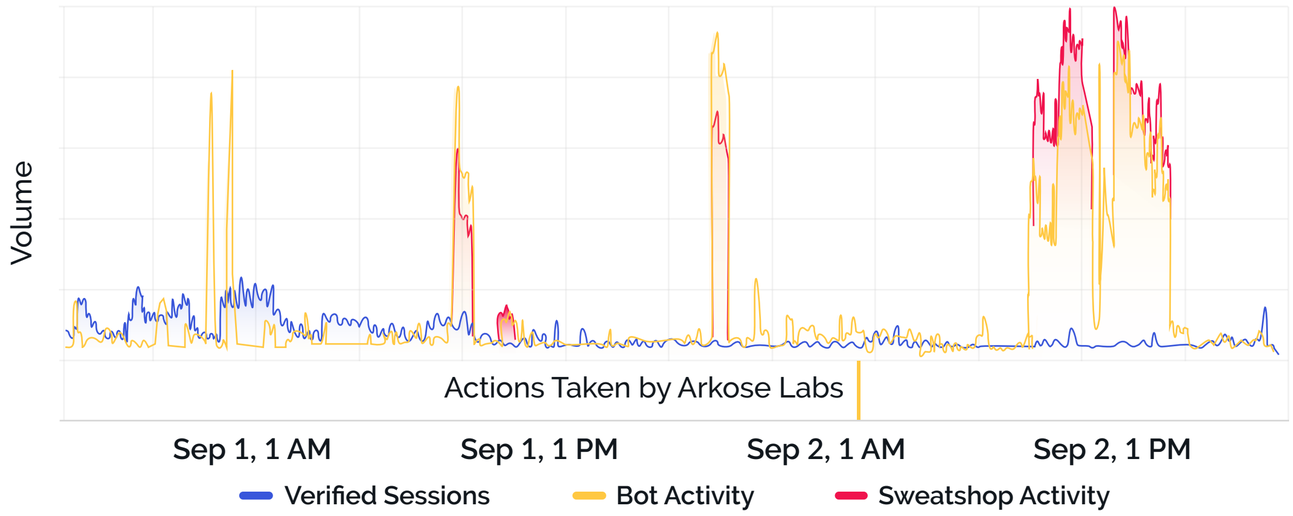
Good customers passed through seamlessly whereas suspicious traffic was shown an advanced challenge designed to stop bots and waste the time of human fraudsters.

This resulted in an increased cost to fraudsters in attacking the platform, which diminished their ROI leading to the long-term mitigation of attacks. This allowed the gaming company's internal fraud team to be freed up from constantly fending off attacks and work more efficiently.

~60% reduction in daily compromised accounts

Enhanced analytics and visibility into downstream fraud signals

Reduced burden on internal teams



Technology Platforms Q3 2020 Attack Trends

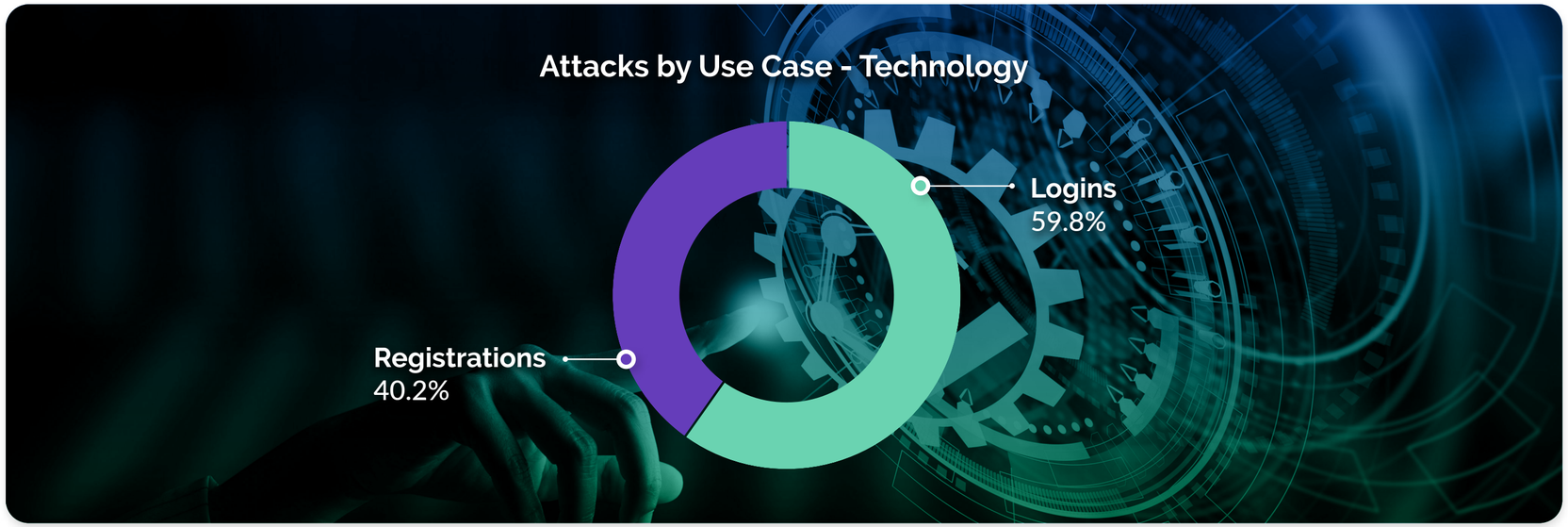
8%
attack rate

14% of attacks from sweatshops

27.5%
mobile vs desktop

Like gaming, technology platforms have seen a massive spike in traffic as the pandemic changed the way people live and work. Cloud-based video platforms, information sharing tools and collaboration platforms have powered the recent move to remote working and virtual education.

Compared to online gaming, however, technology platforms see much fewer attacks despite their newfound popularity. This industry only saw an 8% attack rate. The majority of that was automated, with only 14% of attacks originating from sweatshops. Attacks still mostly came from desktop environments, however the mobile attack rate is above the cross-industry average for the quarter with 27.5% of attacks originating from mobile.



Weekly Attack Trends on Technology Platforms

The quarter started relatively quiet on the attack front in the technology sector. However, the attack rate did increase as the quarter went on, with a noticeable spike in the second half of August. This could have been due to fraudsters targeting virtual education environments as schools started back up. In fact, the move to online education has spurred on cybercrime in this sector. For example, at least 60 school districts have been targeted by ransomware attacks, with hackers demanding money or else publishing the personal information of students.

Conclusion

COVID-19 has sent the world into turmoil, and upended digital traffic patterns, with long-lasting consequences. "Normal" behavioral patterns online are no longer applicable. Which means that the old fraud modeling frameworks are undermined. Companies simply can't rely on formerly true maxims: for example gaming companies are seeing levels of traffic every day that they previously only saw on weekends and retailers are dealing with holiday-levels of traffic on a daily basis.

Fraudsters also continue to get more sophisticated as time goes by, launching intricate attacks that utilize both advanced bot technology as well as humans. Many are using this increased level of digital traffic to also more effectively "blend in" with good traffic and carry out attacks undetected. For businesses, it means that the level of vigilance needed to successfully identify and stop fraud is higher than possibly ever before.

This will continue to be the "new normal" even years from now, when Covid-related lockdowns are but a distant memory. Habits, once formed, are difficult to let go and much of the world's population has gotten into the regular habit of conducting commerce, school, work and even socializing in a virtual environment. This means fraud teams must be able to quickly cut through the noise and spot even the most subtlest sign of attacks, and use targeted friction to deter malicious activity long term.

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