Arkose Labs

Q2 2021
FRAUD & ABUSE REPORT

Insights from the Arkose Labs Global Network

The New Face of Fraud

As we progress into 2021, overall fraud attack rates have leveled off from the pandemic-fueled highs of 2020. But that doesn't mean businesses can rest easy. Fraudsters continue to be innovative and opportunistic and continue to target new avenues for monetization and deploy tools and strategies with ever-increasing sophistication.

In addition to the evolving tactics and attacks of professional fraudsters, businesses have to be aware of an increasing segment of so-called "regular users" that are engaging in abusive activity.

These are people who dabbled in fraud in 2020 -- many due to suddenly being plunged into financial hardship due to lockdowns -- and have continued to find the profession profitable and continue on with it instead of returning to legitimate work. And there are also a growing amount of people who, while not pursuing fraud as a full time job, are engaging in activities like fake reviews, disseminating fake information on social media and bonus abuse. This "new face of fraud" has now become a permanent part of the landscape, and it is difficult to detect and stop.

So while fraud attack volumes have abated somewhat, diversifying attack types continue to be a major issue for industries across the board. As always, it will take a unified effort from all of us in the fraud prevention and security ecosystem to successfully stop these attacks.

Kevin Gosschalk

Founder and CEO

Fraudsters continue to be innovative and opportunistic and continue to target new avenues for monetization and deploy tools and strategies with ever-increasing sophistication.

Top Trends at the Beginning of 2021

Increase in Human-Driven Fraud

Q1 saw a marked increase in human-based attacks, especially in tech and media. This highlights the continuing importance of human-driven fraud in successfully carrying out attacks.

Drop in Attack Rate from Q4

2021 started like the previous year ended, with high attack levels.. At its peak, the suspicious traffic rate was 30%, but went down to a more manageable 17% by the end of Q1.

Rise in Malicious Mobile Traffic

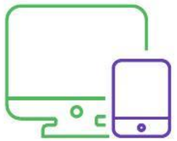
Higher levels of fraud originated from mobile devices in Q1, up to 28% of all attacks compared to 16.2% last quarter. This speaks to the importance of protecting the entire digital perimeter.

A Diversification of Attack Types

While 2020 was dominated by ATOs and login-based attacks, Q1 2021 saw a significant uptick in bot attacks for things like spam, info scraping, in-game abuse, inventory hoarding & API abuse.

The Rise of the Cyborgs

The increase in humans launching attacks speaks to the increasing relevance of so-called "cyborg" attacks — with fraudsters deploying a mix of bots and humans to successfully pull off attacks.



Attack of the Smart Devices

In a continuing effort to blend in and appear as legitimate traffic, fraudsters are hijacking the trove of new IPs associated with IoT-connected devices. These IPs are often from a geography not typically known for fraud attacks, such as North America.

Q1 2021 in Review

Q1 Attacks

17%
Attack Rate

15 Million Daily Attacks in the Busiest Weeks of Q1

Humans vs Bots

13.4%
Humans

86.6%
Bots

2X Volume
of Human-driven Attacks

Mobile vs Desktop

28%
Mobile

72%
Desktop

9% Increase
in Mobile Attack Rate

Regional Trends

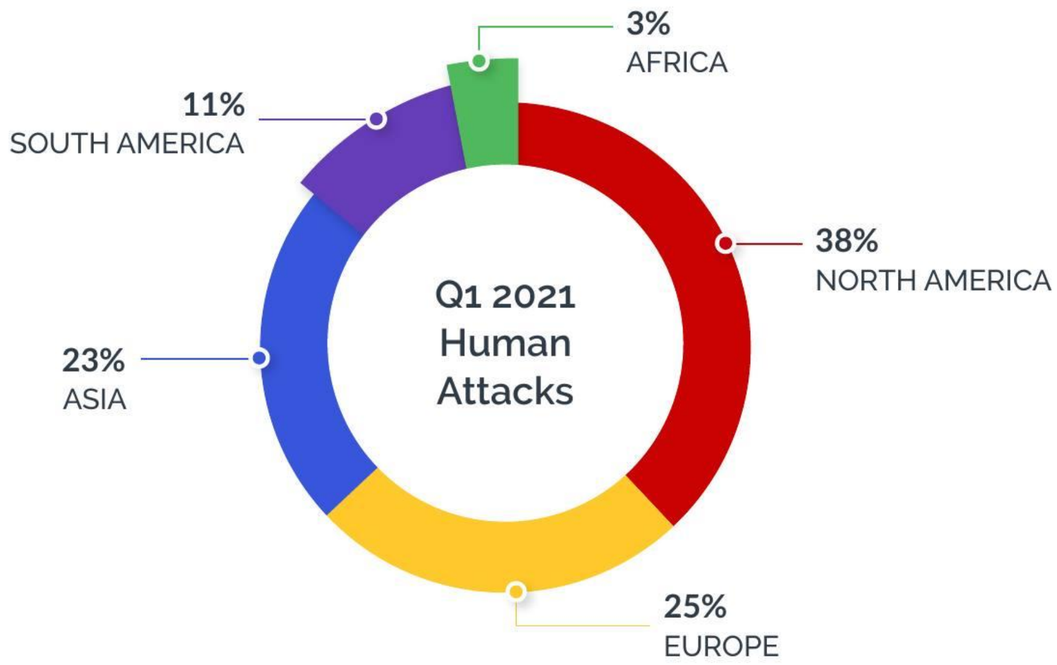
⅓ Attacks Originate from Europe

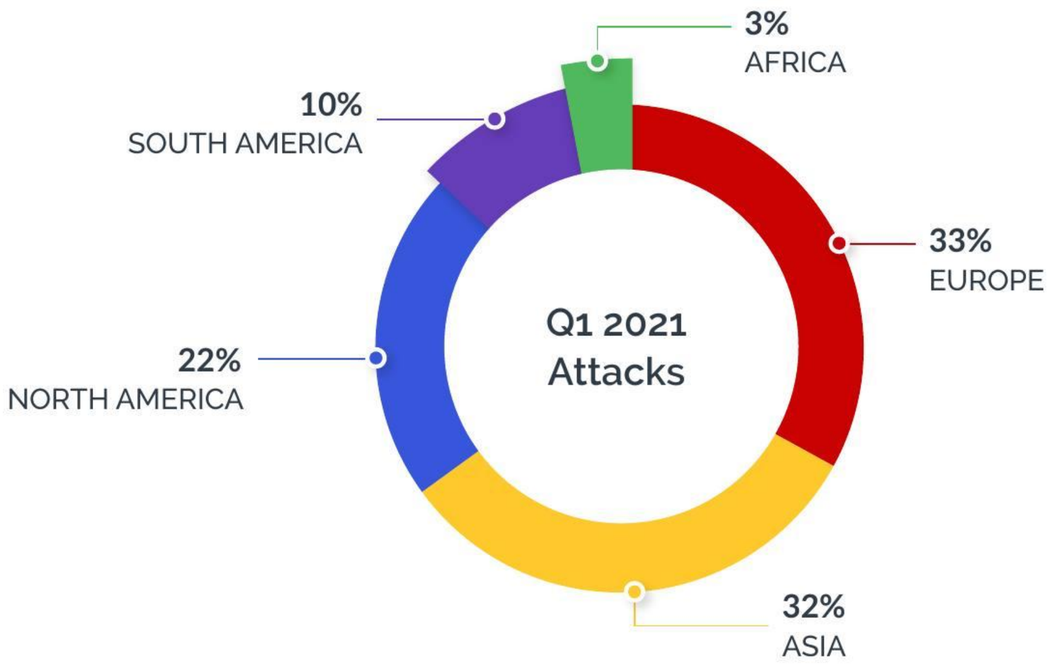
USA and Russia
Top Q1 Attacking Countries

Q1 Attacks By Region - Europe Takes the Lead

There were similar levels of attacks originating from Europe and Asia in Q1 2020, with Europe the top attacking geography, with over one third of all attacks. This is largely influenced by the consistent high attack levels seen emanating from Russia.

One noteworthy trend from Q1 was the large amount of human-driven attacks from North America - primarily driven by attacks on social media companies. Humans are required to launch scams on these platforms, which they do by sending phishing messages or malicious links to good users seeking to place malware on their devices or extract sensitive information, which can then be resold at a large profit.



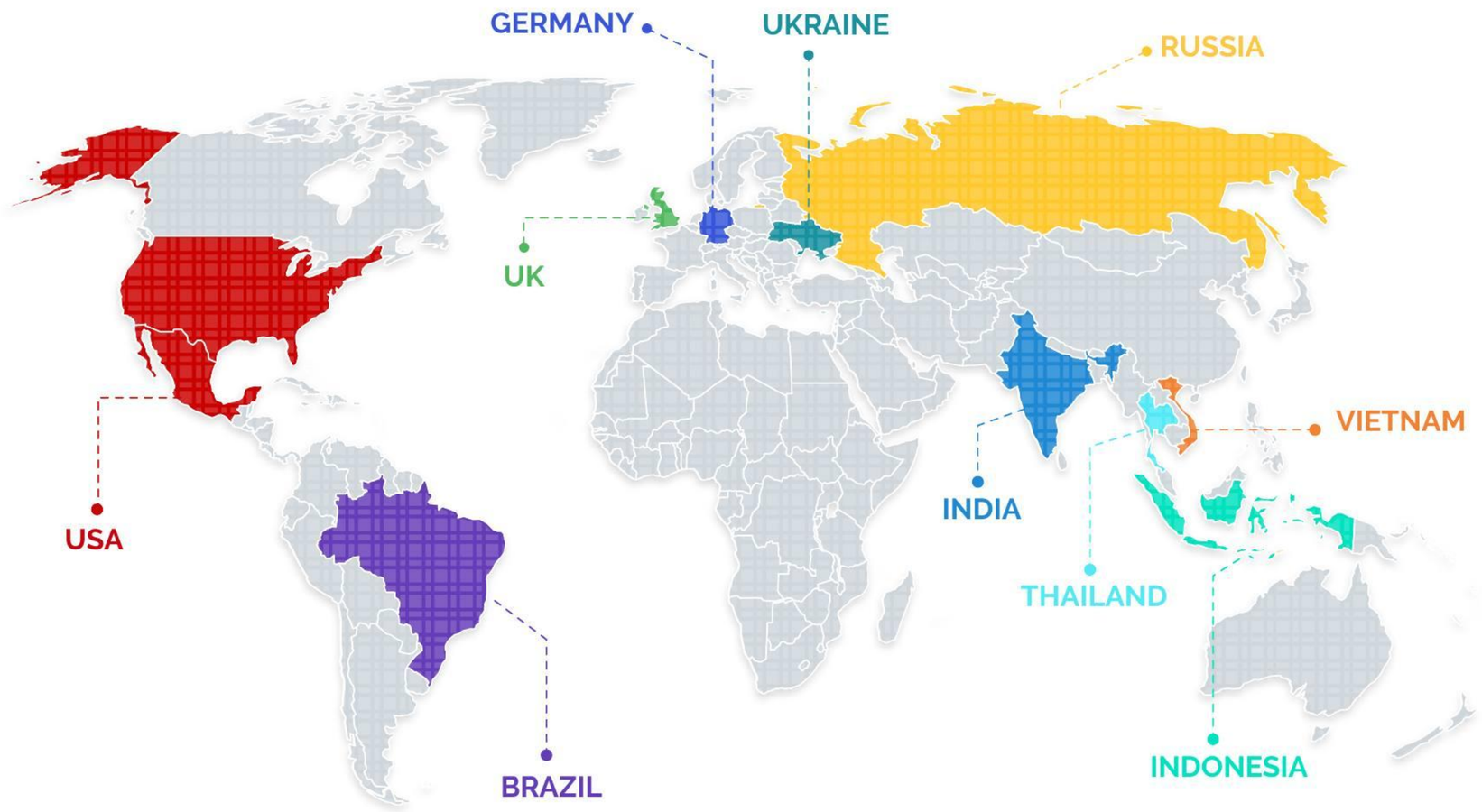


Q1 Top 10 Attacking Countries

The USA and Russia were the top attacking countries, with roughly similar volumes. While Russia is generally always near the top, the US rose from 5th in Q4 2020 to the top spot in Q1 2021

However, it should be noted this was not necessarily due to a marked increase in attacks stemming from the US, but rather a decrease in attacks from more traditional fraud hubs such as Vietnam, Brazil and Indonesia.

New countries in the top 10 during Q1 2021 include several from Europe, including the Ukraine, the United Kingdom and Germany. Overall, attacks were down across most geographies during Q1 as compared to Q4 of 2020.



Is Your Smart Refrigerator Committing Fraud?

Recently, there has been a rise in an insidious new trend of bad actors hijacking trusted IP addresses to carry out attacks, to help avoid detection. This has been made easier by the explosion of new IPs created in recent years due to a proliferation of smart devices and the IoT.

Cybercriminals can hijack IPs by rerouting Border Gateway Protocols(BGPs) which are the standard routing protocol of the internet. This allows bad actors to take over IP addresses by compromising routing tables. The explosion of internet connected devices in homes over the last several years — including home security devices, virtual assistants and smart appliances — has now provided fraudsters and other attackers with loads of new IPs to potentially hijack and misuse.

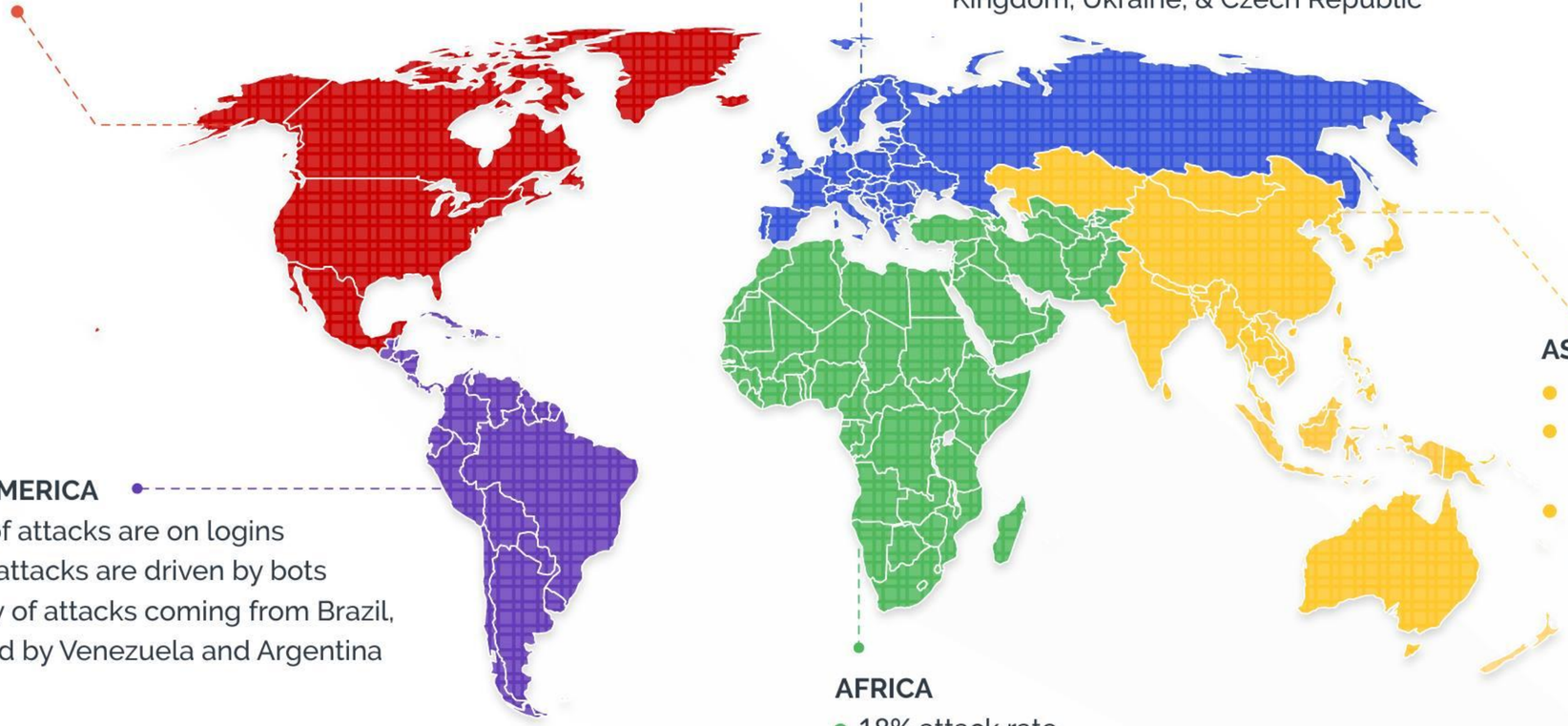
Those intent on large-scale cyberattacks can, for example, use a network of these compromised devices to launch a DDoS attack against a website or series of websites. But fraudsters can use them too, by spoofing or hijacking these IPs to appear as “good” traffic that has previously been seen and verified by a particular digital platform before then committing any number of fraud attacks against a business or user.

This makes it difficult for businesses that rely very heavily on IP reputations for fraud decisioning, as more traffic falls into the nebulous “gray area” that doesn’t explicitly appear good or bad. Businesses need secondary screening to accurately test potentially suspicious traffic and ensure good users aren’t blocked and fraudsters are kept out.

Q1 2021 Regional Attack Trends

NORTH AMERICA
- 37.7% of all payments are an attack
- 1 in 2 travel transactions is an attack
- One in five media transactions is an attack

EUROPE
- 19.3% attack rate.
- 88.1% of attacks are bot-driven
- Top attackers: Russia, Germany, United Kingdom, Ukraine, & Czech Republic



ASIA PACIFIC
- 39.5% of attacks on logins
- Nearly 2 in 3 transactions in retail is an attack
- Top attackers: Vietnam, India, Indonesia, Thailand & China

SOUTH AMERICA
- 51.3% of attacks are on logins
- 83% of attacks are driven by bots
- Majority of attacks coming from Brazil, followed by Venezuela and Argentina

AFRICA
- 18% attack rate
- 40% of attacks on logins
- Top attackers: Northern Africa (Egypt, Morocco, Algeria & Nigeria) and South Africa

ATO Survey: The Downstream Cost of Attacks

Successful fraud attacks don't just have a one-time cost, which is why businesses must focus on stopping fraud at the earliest possible point.

Arkose Labs recently polled 100 IT executives on how account takeover attacks impact their business, and it's clear successful attacks have a continual downstream cost. These include compromised accounts sending spam and phishing messages, being used to launder money, as well as increased operational costs associated with remediating the problem.

Operational efficiency is also hindered as customer support gets flooded with calls from angry customers, and compliance teams have to deal with any regulatory fallout. Internal fraud and security teams also have to spend more time on manual reviews and fine-tuning systems.

63% of executives said that account takeovers had caused their business compliance concerns.

60% of businesses said that ATO attacks had negatively affected their brand reputation.

49% said they had lost customers in 2020 due to successful ATO attacks that targeted their businesses.

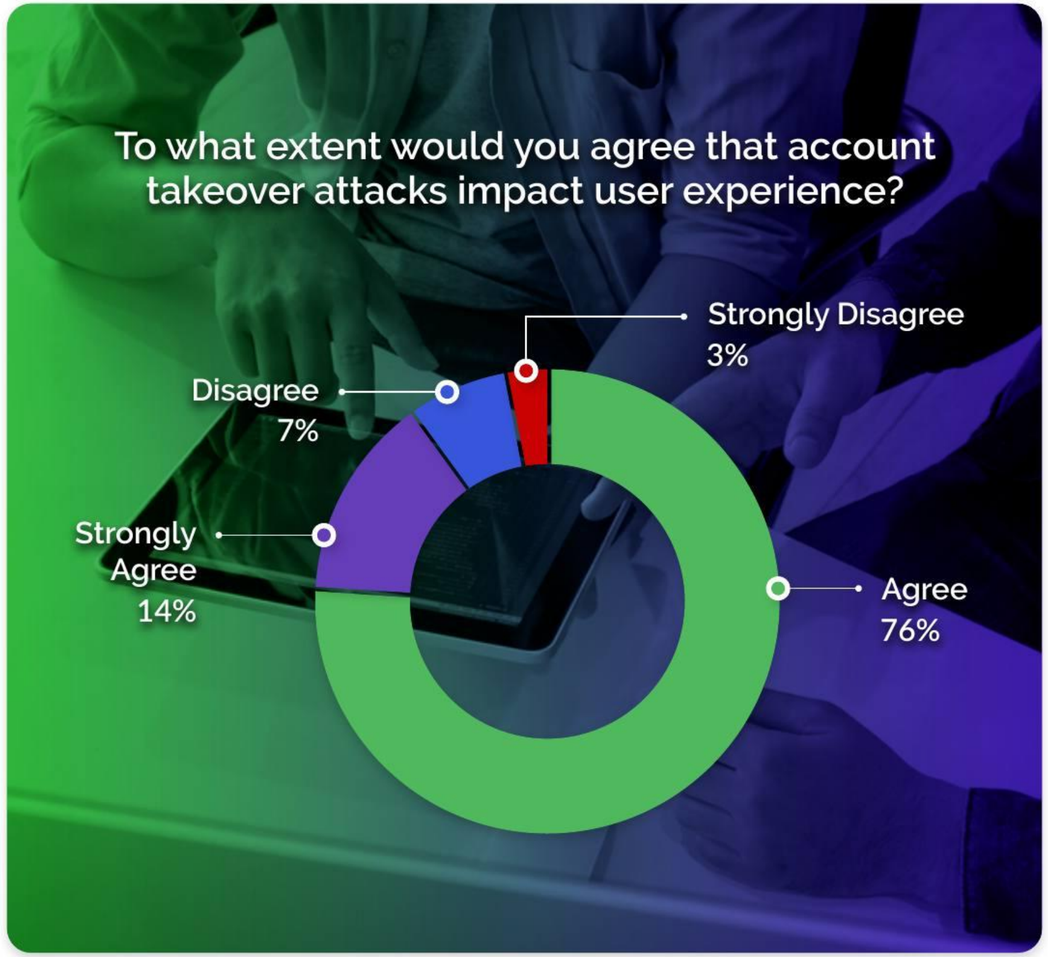
ATO Attacks Severely Impact the User Experience

One thing most businesses agree on is that failing to stop ATO fraud massively impacts the digital user experience.

In our poll, about half of the respondents said that their business had lost customers over the past year due to account takeover attacks. And a full 90% agreed that account takeovers impacted user experience. This is a critical issue because of the time and money spent to remediate compromised accounts and the erosion of consumer trust in companies that could not keep their sensitive data protected.

This can further lead to an impact to brand reputation, as frustrated users flood contact centers with complaints and take to social media to voice their displeasure. It can also affect new customer acquisition, with consumers seeing negative news headlines about data breaches.

It's clear that failing to stop fraud at the digital front end ruins the experience for customers and and leads to loss of revenue and increased costs.

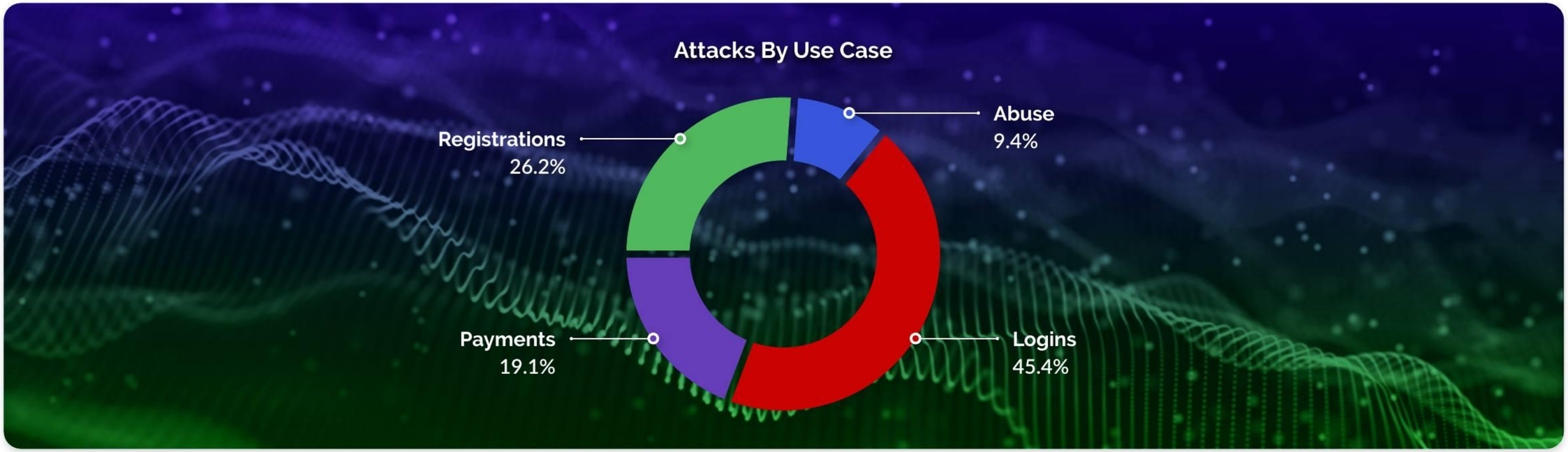


Fraudsters Diversify Their Attack Points in Q1

A noteworthy trend during Q1 2021 was a diversification of attacks across use cases. The last few quarters had seen the majority of attacks focus on logins, with waves of large, sustained credential stuffing attacks.

While login attacks are still high, at 45% of all attacks, there was an increase in the proportion of spam and abuse and payment-related attacks.

There was a 36.1% increase from Q4 2020 to Q1 2021 in abuse - which encompasses scraping, spam & malicious content, inventory hoarding, fake reviews, and bot-driven API abuse. Q1 also saw a 27.6% increase in payment attacks compared to Q4 2020.



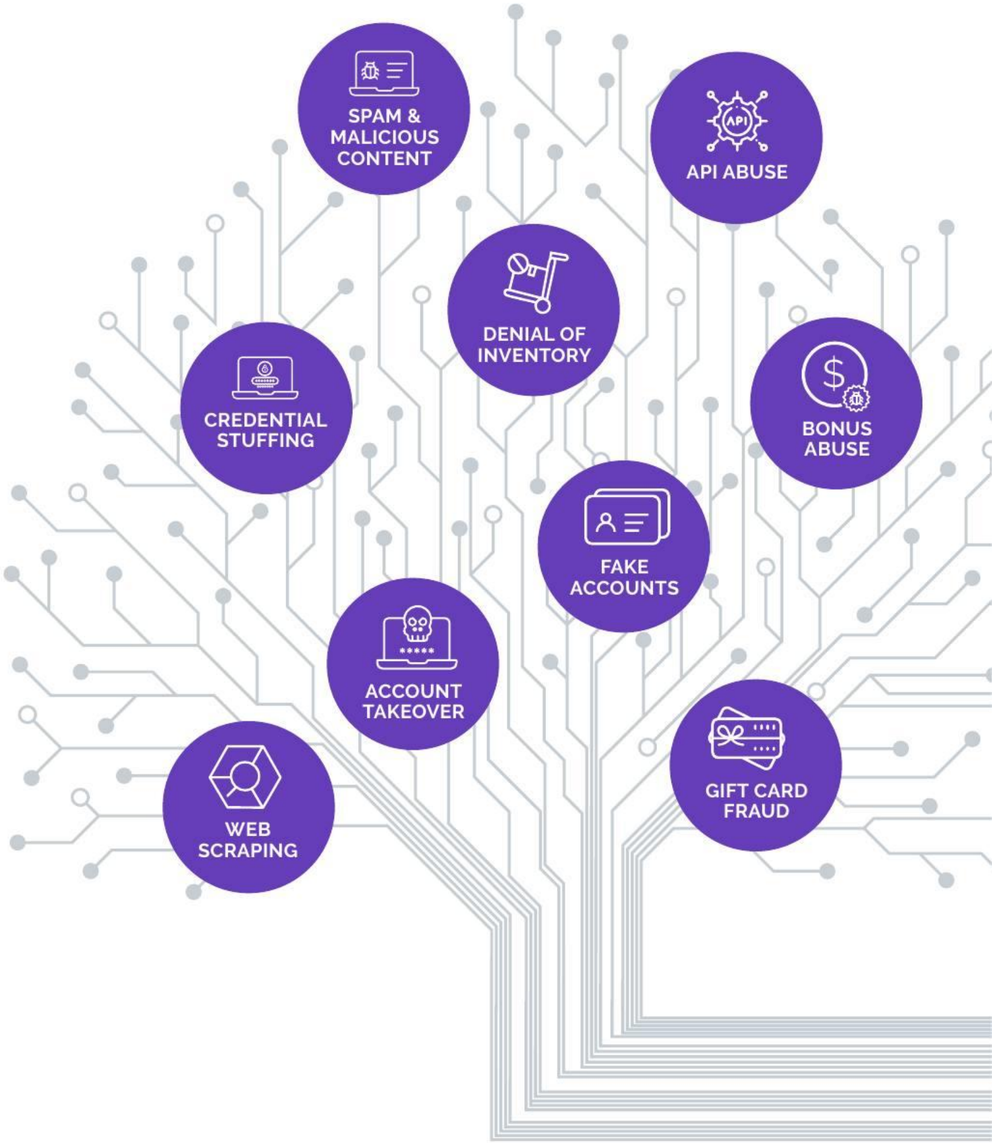
Protecting the Full B2C Perimeter

With consumers interacting with businesses across numerous digital touchpoints, it is imperative to ensure all of these interactions are protected from fraud and cyberattacks. Defending against evolving attacks targeting all these points can get complex, without versatile protections in place that can work seamlessly across use cases.

That's why businesses need to adopt a trust and safety approach that goes beyond traditional fraud mitigation to defend against how fraudsters target and monetize each touchpoint specifically.

With an explosion of mobile and internet connected devices, as well as stolen data, fraudsters have many tools and tricks to blend in with good traffic and appear as if they are good users. It's getting more complicated for businesses to analyze the increase in digital traffic and parse out what is suspicious versus non-suspicious.

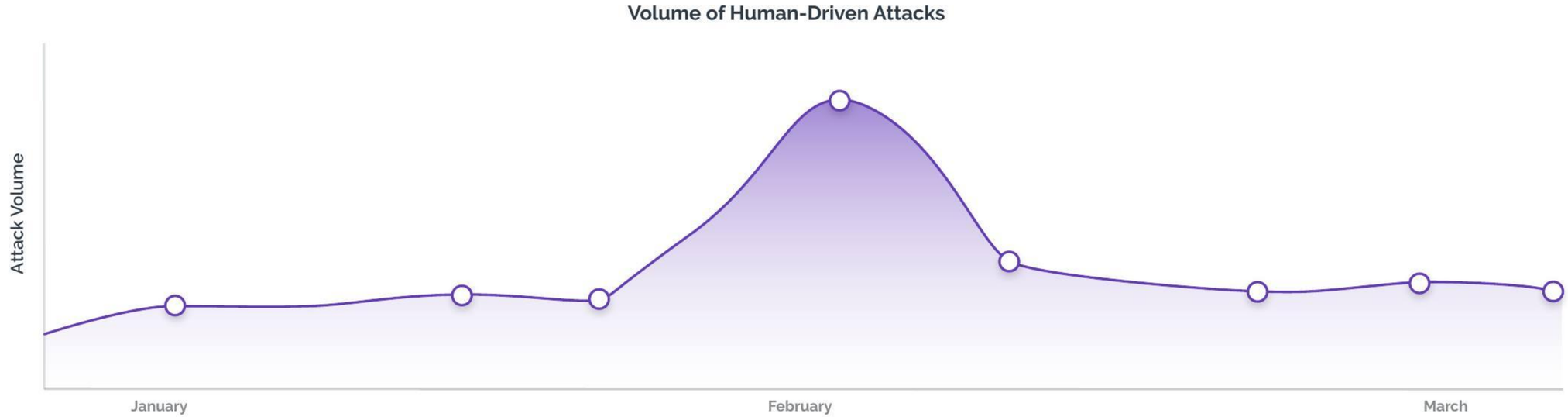
This also has to be done with no discernible impact or disruption to the good end user. This is why effective fraud solutions made for today's always-on digital world must be designed from the outset with UX in mind as well as fraud prevention and security protocols.



Human-Driven Attack Volume Doubles From Q4

One surprising trend that was detected in Q1 was a significant rise in human-driven fraud. The attack volume originating from human fraudsters doubled Q1 2021 as compared to Q4 2020. In particular, there was a distinct spike in human-driven attacks starting in the middle of the quarter. This varied by industry with tech (40%) and media (32%) seeing the highest human-driven fraud. Human fraud also spiked in payment attacks on retail companies.

This trend illustrates how important humans are to carrying out attacks. These are organized operations of workers that are deployed to attack at scale while keeping costs low and circumvent anti-bot defenses. This trend could also indicate many of those who turned to fraud after sudden job losses during the pandemic may have found this new line of work was profitable and continued doing it.



Case Study: Arkose Labs Helps Telecom Stop Hybrid Human & Bot Attacks

Business Problem

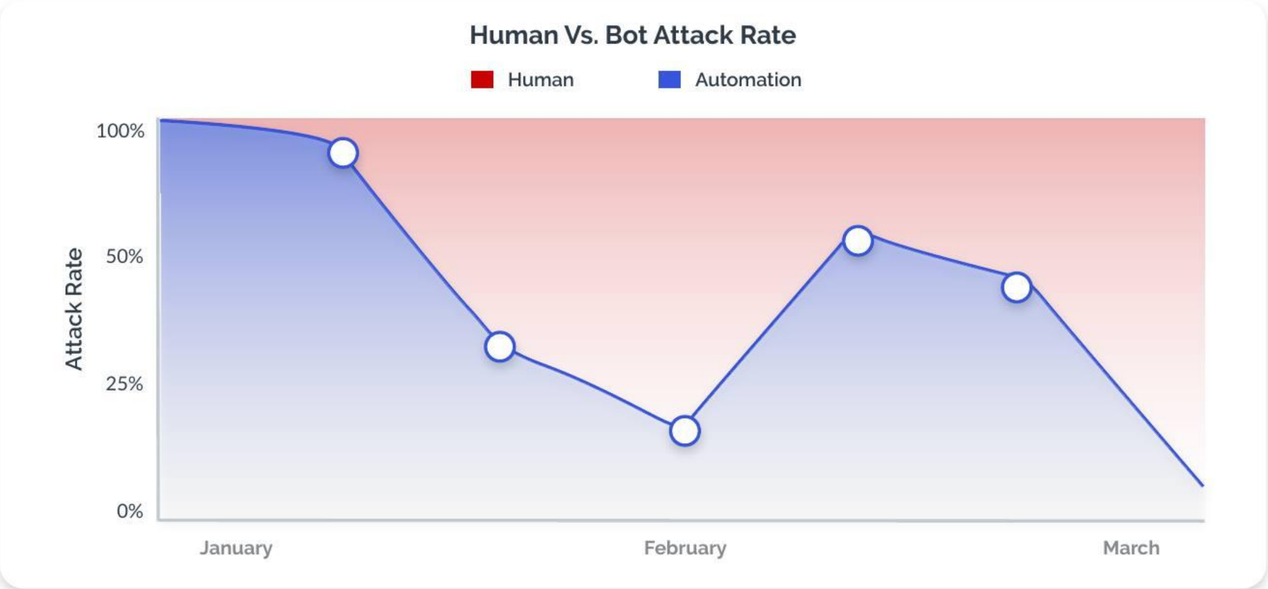
The client, one of the world's biggest telecom companies, was dealing with persistent, large-scale bot attacks. These attacks were targeting the login flow to compromise user accounts, as well as creating fake new accounts at scale to take advantage of new customer promotional offers.

Solution

Arkose Labs was deployed on both the registration and login pages and immediately the automated attacks almost entirely stopped. However, fraudsters behind the attacks quickly pivoted after the automation was stopped and then the company started seeing a rise in human-based attacks coming from fraud rings. Enforcement challenges designed to slow down and frustrate human fraudsters were served, which wasted their time until they were compelled to stop attacking.

Results

Over the course of a 30 day period, Arkose Labs detected and stopped more than 4 million attacks coming to the client's login and new account registration flows. Arkose Labs also worked with the client to deliver customized enhanced analytics through the customer dashboard that enabled the client to gain greater insights into fraudulent activity and helped them make more accurate decisions on dealing with downstream fraudulent activity.

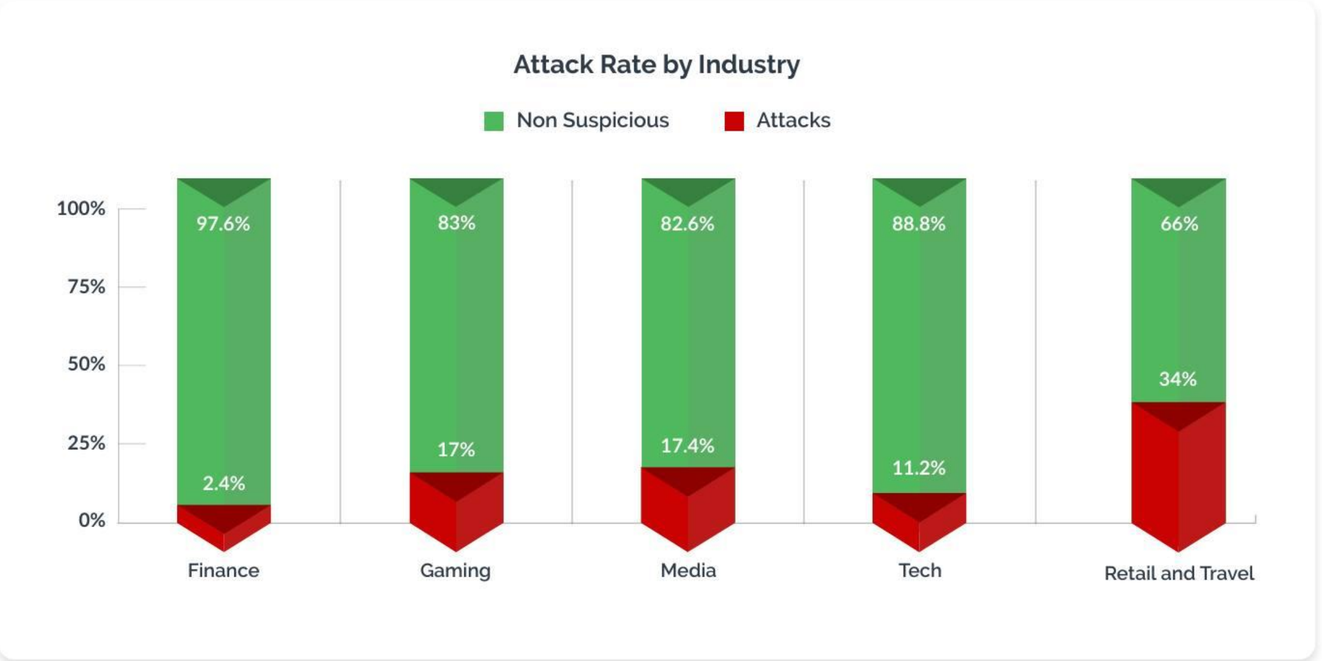


Retail Sees Highest Attack Levels in Q1 2021

Throughout 2020, it was the gaming industry that had seen the highest levels of fraud. This was due to a massive influx of new customers flocking to online gaming platforms during lockdowns and the subsequent rise in fraudsters targeting these new accounts.

However, the beginning of 2021 has seen a bit of a shift, with online retail now seeing the highest attack rate among all industries. A little more than 34% of digital traffic to retail and travel sites was identified as malicious.

Retail was also highly attacked during Q4, which makes sense because that time period encompassed Black Friday and the holiday shopping season. It's interesting to see this trend continue into Q1, which could indicate the rise in ecommerce traffic in 2020 — especially from digital debutantes forced online by the pandemic — has become the new norm.

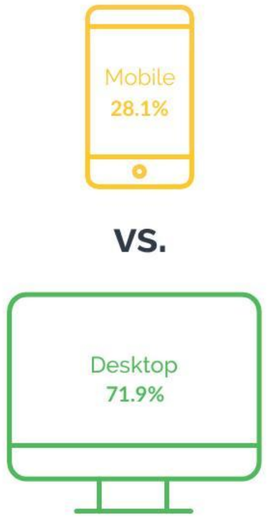


43% Increase in Mobile Attack Rate in Q1 2021

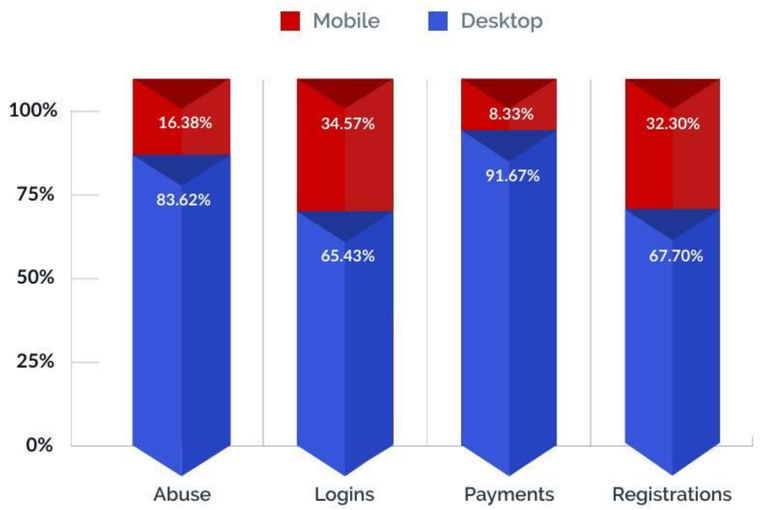
Mobile continues to increasingly become a more prominent channel in launching fraud attacks. In Q1 the mobile attack rate was 28%, compared to 19% last quarter. These attacks are primarily focused on the login and new account registration flow. Gaming was the top sector targeted by mobile-based attacks.

A major reason why attacks originating on mobile devices are increasing is because of the increasing popularity of this channel with consumers. With more and more good users interacting with businesses via mobile devices, fraudsters can more easily hide their tracks. Mobile devices can be spoofed, and there are numerous websites where fraudsters can purchase not only IP addresses, but the appropriate mobile device fingerprint that goes with it.

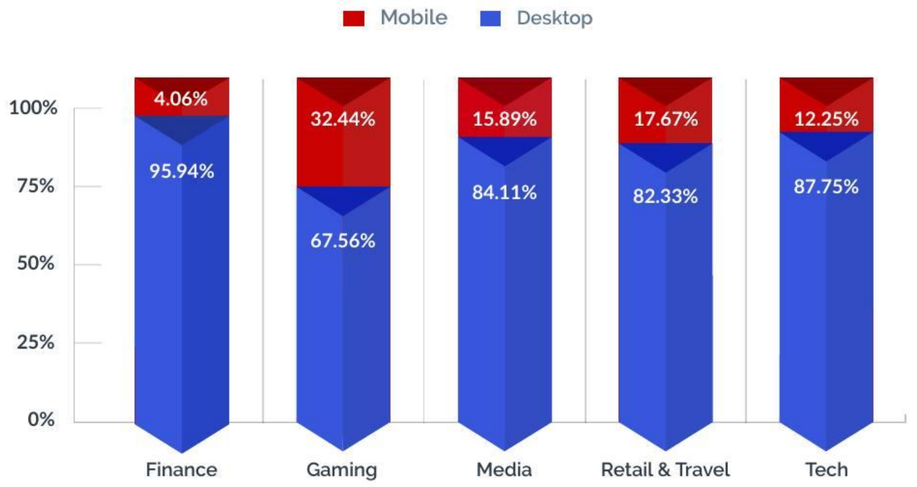
Q1 Attacks by Device



Desktop vs Mobile Attack Rate by Use Case



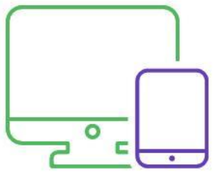
Desktop vs Mobile Attack Rate by Industry



Financial Services Faces Sustained Attacks Targeting Loan and Credit Applications

2.4%
Attack Rate

11% Increase in ATO Attacks



4.1%
Mobile vs Desktop Attack Rate

Financial services continue to see a steady stream of fraud attacks targeting new loan and credit applications. This is a trend that continues on from 2020, when fraudsters flooded digital banking channels to take advantage of government programs designed to help businesses (such as PPP loans), as well as using synthetic identities to take out personal loans with no intention of repaying them. As fraudsters realized the success they could have with loan application fraud during the initial stages of the pandemic, they have continued to target this area.

Financial firms also saw an 11.2% increase in login attacks in Q1 compared to Q4, as fraudsters increasingly target valuable financial accounts with ATO attacks.

Application Fraud in Financial Services

Loan Applications

Money Mule Accounts

Credit Cards

Payment Protection Program Fraud

Banking Case Study: Neobank Stops ATOs with Arkose Labs

Business Problem

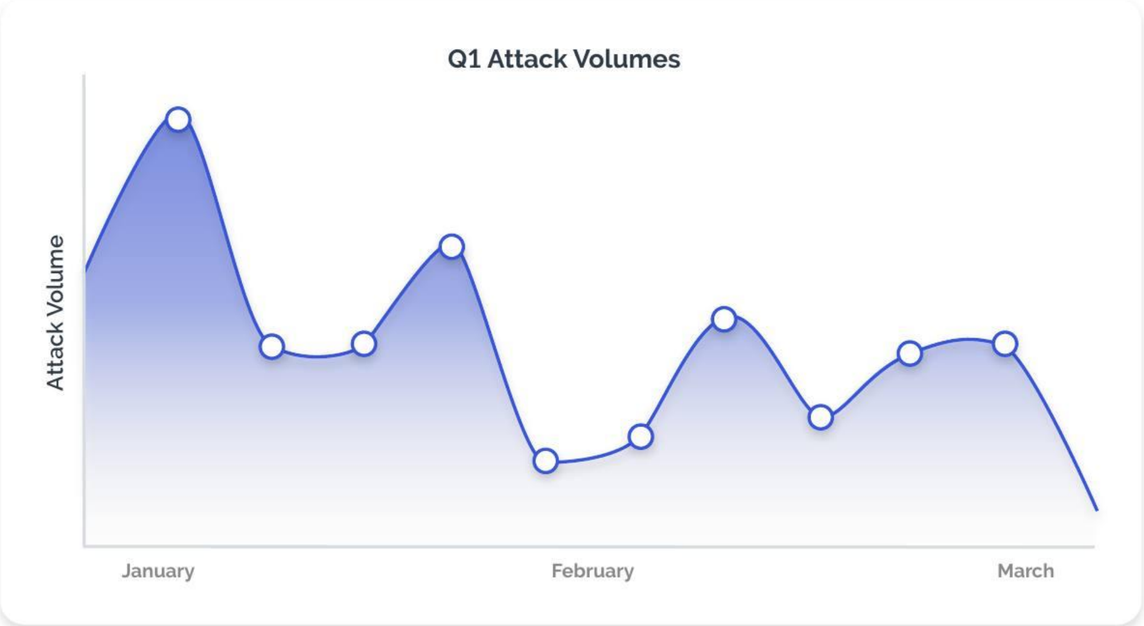
A global fintech was seeing nearly 30,000 credential stuffing attempts a day, with attackers looking to hack into valuable user accounts. Fraudsters would deploy bots that would directly target the back-end APIs. By by-passing web forms, fraudsters could write simpler scripts that would allow them to carry out attacks at greater volume and velocity, putting more accounts at risk.

Solution

The fintech implemented the Arkose Labs Fraud & Abuse Platform to protect its login forms and backend APIs. Arkose Labs monitors all traffic for known signals of abuse, using behavioral fingerprints, velocity, and rate monitoring, and a proprietary user IP database. Arkose Labs uses dynamic tokens to verify that traffic is passing from client to server and not targeting APIs directly. The platform uses a proprietary enforcement challenge that cannot be solved by bots.

Results

After implementing the Arkose Labs platform, the fintech saw a more than 75% reduction in these attacks. Furthermore, it realized cost savings of $100k per month related to remediating compromised accounts.



Big Spike in Mobile-Driven Attacks on Gaming Companies

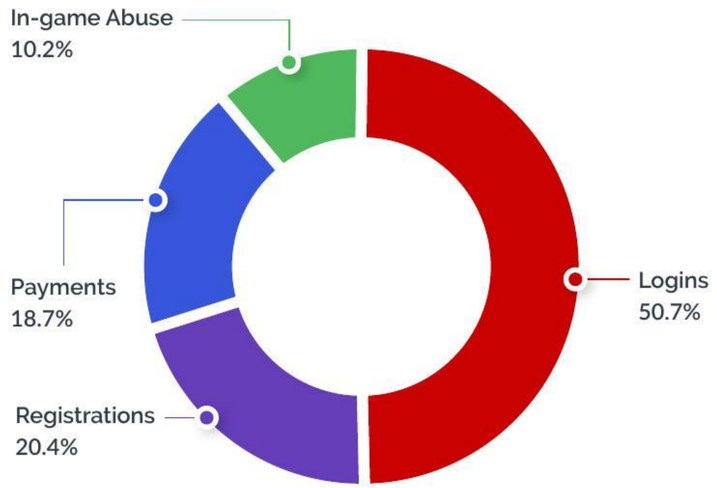
17%
Attack Rate

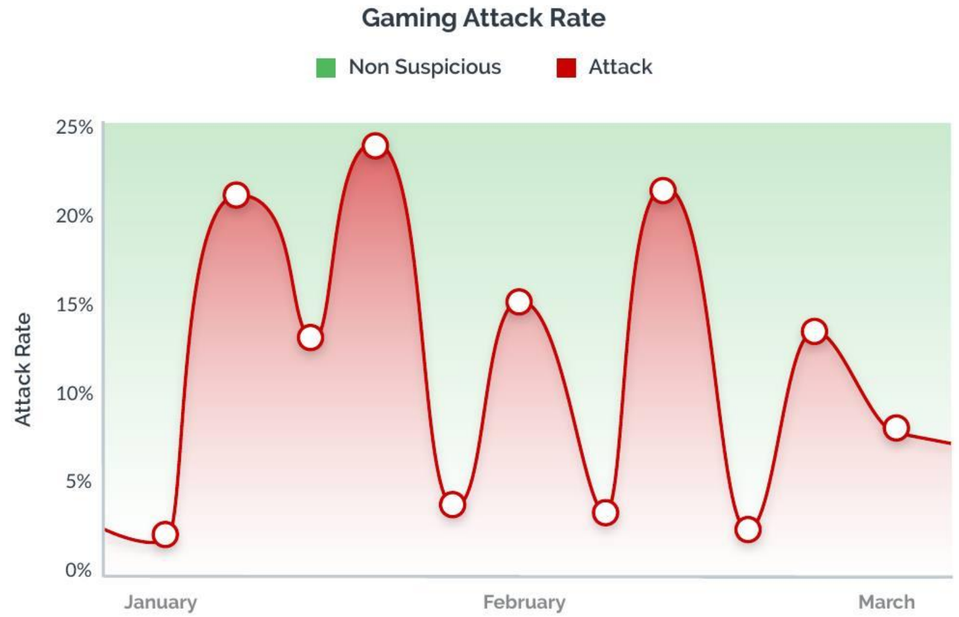
96.6% Bot vs Human Attacks

32.6%
Mobile vs Desktop

Gaming — the most attacked industry in 2020 — saw high rates on mobile attacks across all touchpoints during Q1. Overall, attacks from the mobile channel increased from 19% in Q4 to 32% Q1 2021. These attacks are still overwhelmingly bot-driven, with nearly 97% of attacks being automated.

While logins remained the top attack touchpoint in Q1, there were more evenly distributed attacks in Q1 than previously seen, with less sustained ATO and credential stuffing attacks and a more normalized attack pattern.





Profile of a Gaming Fraudster

Fraudsters in the online gaming space are not your typical criminals. Many are teenagers who themselves play these games and are looking for an advantage. Gaming is also a popular "starting off" point for burgeoning fraudsters, since they use simple bots to launch attacks at scale and there are many gray market forums to easily resell in-game digital items and currency.

OCCUPATION
Fraudsters

POSSIBLE LOCATION
Vietnam, Brazil, Russia, Indonesia, or India

STATS

- Playing Volume = High
- Win Rate = <5%
- ROI = High

CHARACTERISTICS

- Target = Narrowly Focused
- Platform Knowledge = Expert
- Maneuverability = High
- Fear of Consequences = None
- Playing style = Devoted to Winning

POWER UPS

- Data Brokers
- Identity Farms
- Human Sweatshops
- Money Mules
- Arms Dealers
- Marketplace
- Infrastructure Providers
- Coders

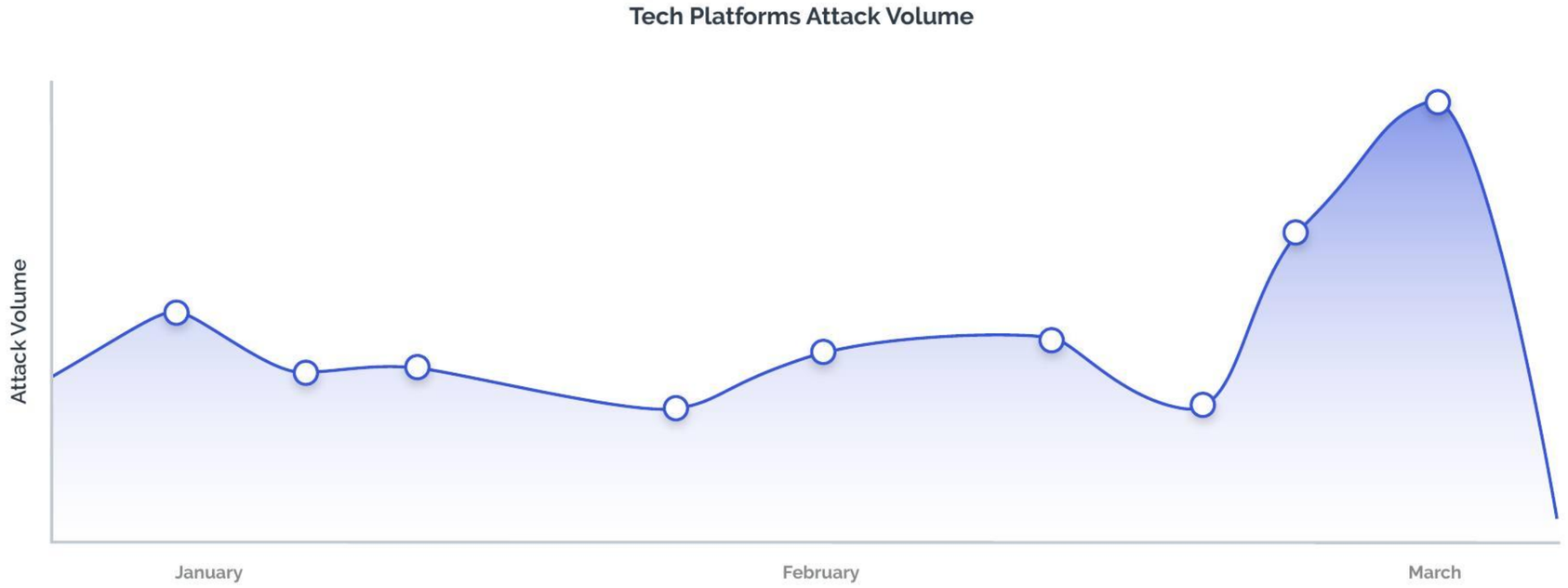
Tech Platforms: A Wide Variety of Attack Types and Monetization

11.2%
Attack Rate

40.4%
Human Attack Rate

12.3%
Mobile vs Desktop

Tech platforms see a bit of everything when it comes to fraud attacks, as criminals utilize a variety of tactics to launch and monetize attacks in this industry. There was a noticeable spike in Q1 of human-driven attacks on the new account sign up flow. One example of this is fraudsters signing up for fake new accounts on a cloud storage and collaboration platform in order to get free promotional server time. Attackers will normally then use the free server time to mine bitcoin or other cryptocurrencies. With a human attack rate of more than 40%, tech platforms see some of the highest ratios of human-driven attacks, again reflecting the more intricate and varied ways that fraudsters target these platforms.



Media Companies Targeted to Facilitate Human-driven Scams

17.4%
Attack Rate

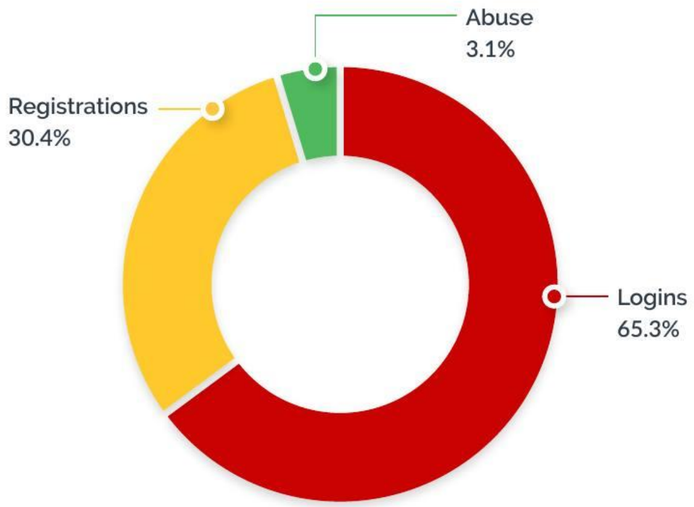
31.8%
Human Attack Rate

12.3%
Mobile vs Desktop

Media companies — defined as dating, social, and streaming sites — are often used to launch human-driven fraud and abuse. For example, human fraudsters set up fake accounts on dating and social media sites to then send phishing messages or romance scams to unsuspecting good users. This is a big reason why fake new account fraud increased drastically in Q1 for this sector.

The attack levels for streaming companies are not so high, but they face unique challenges in extending security to a variety of smart devices customers regularly use to consume streaming content.

Attacks by Use Case - Media



Media Attack Volume

Case Study: Major Travel Site Slashes Bot Traffic

Business Problem

The client operates one of the world's foremost search engines for travel and booking, for both consumer as well as business travel. For this company, the "look-to-book" ratio is one of their key performance indicators. This critical travel industry metric shows the percentage of people who visit a travel website or mobile app compared to those who actually make a purchase. The company is contractually bound with many of its providers within the airline and hospitality industry to maintain a certain ratio. However, when millions of bots set out to scrape information off their site, it damaged their ratio, as well as greatly strained their IT infrastructure.

Solution

The Arkose Labs Fraud & Abuse Platform was implemented on new user registration and login flows, as well as the company's search API, which bots were directly targeting. Arkose Labs detected this automated traffic coming to the site and served it with a proprietary enforcement challenge designed against automation.

Results

The company had been seeing 35 million malicious bots hit their site per day; after implementing Arkose Labs that number was reduced by more than 99%. This enabled the client to raise its look-to-book ratio from around 1 percent to more than 6 percent, a significant increase that pleased its providers. It also was able to ease pressure on its server usage, as millions of sessions daily that were initiated by malicious bots were eliminated.

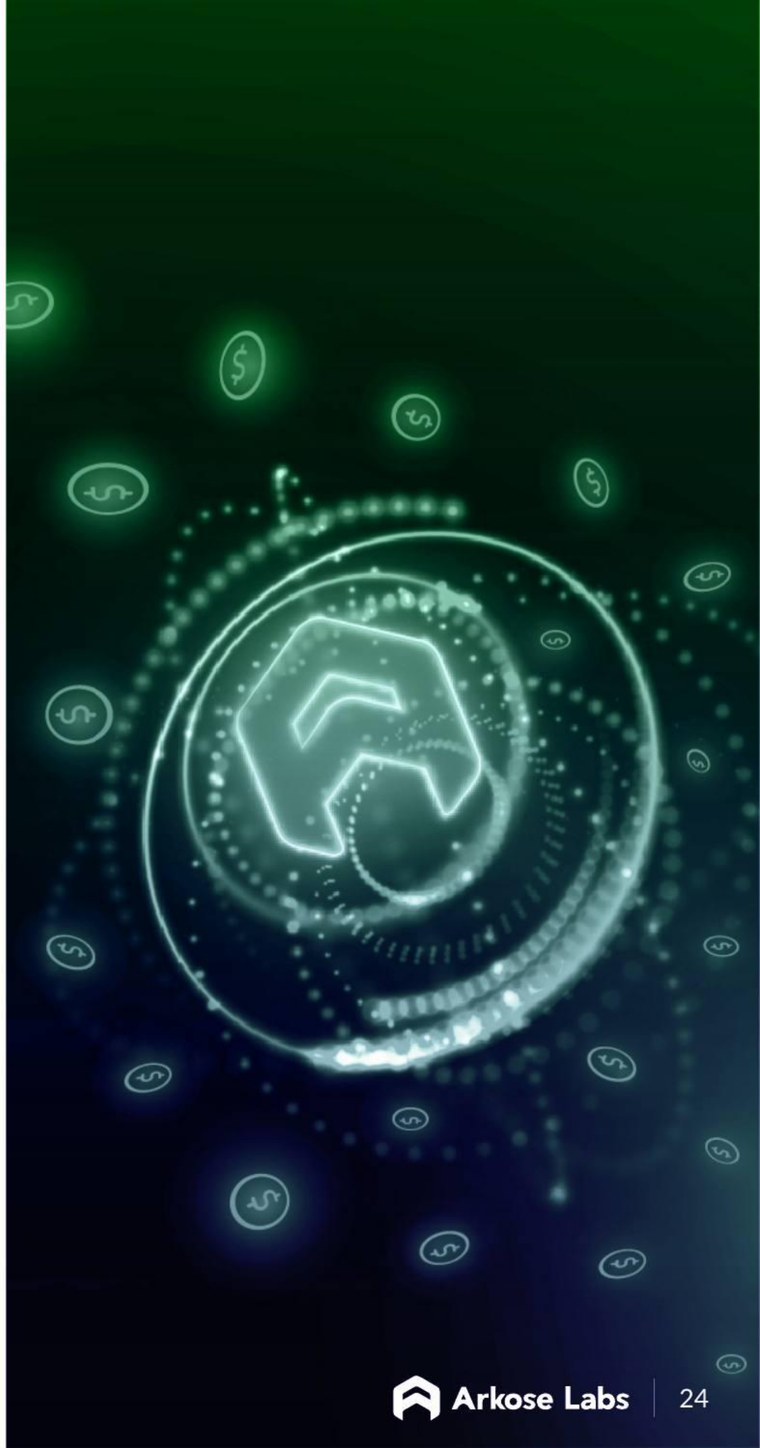
Conclusion: The Fraud Landscape Never Stands Still

A major lesson of the Covid-19 pandemic and the associated fallout is that fraudsters are innovative and quick to adapt to new and changing circumstances.

Fraudsters quickly took advantage of lockdowns and the shift to digital last year to power-up their attacks. We've also seen how some people who never previously dabbled in fraud but did so during the pandemic realized there was money to be made and are continuing to do so in small amounts. This could include creating fake accounts to obtain new user sign-up bonuses on online gambling sites, or using bots to reserve and buy in-demand items — such as new video game consoles or limited edition sneakers — to then resell at a profit.

That's why it is more important than ever before that all digital businesses have fraud defenses in place that effectively stop fraudsters before they can get in and wreak havoc on a business and its users. This is akin to having a strong lock on your front door and a robust alarm system; it's easier to simply keep the bad guys out in the first place rather than try and clean up the mess afterwards.

By doing so, fraudsters will be unable to make money from the myriad of downstream abuse they engage in after initially breaching a business's defenses, and we can help create a safer internet for all.



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
arkoselabs.com

Offices

San Francisco
250 Montgomery St 10th Floor, San

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo