Arkose Labs

2021
STATE OF FRAUD AND ABUSE IN GAMING

An Arkose Labs Industry Report

Fighting an Invisible Enemy

The gaming industry had quite a year in 2020. When the world was suddenly thrown into lockdown due to the Covid-19 pandemic last spring, millions flocked to online gaming platforms as a vital means of entertainment. Gamers who normally only played on the weekend began playing every day, and many who had never played before flocked to online gaming platforms as a way to connect with others and pass the time.

Unfortunately, fraudsters also saw this opportunity and responded in kind. As millions of homebound people played games in far greater numbers than ever before, fraudsters targeted this massive increase in traffic. The overall spike in traffic created an opportunity for fraudsters to “blend in” and go unnoticed. Furthermore, many previously law-abiding gamers began to dabble in fraud as they saw a means to hack in-game environments, steal digital items and currency, and manipulate online auction houses. This difficulty in detecting fraud was akin to fighting an invisible enemy on the battlefield.

Gaming was the most attacked industry in 2020, but fraud have off somewhat at the beginning of 2021. While logins remained the top attacked 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.

Still, gaming platforms must remain vigilant; this industry remains a high target for fraudsters since most user accounts are less secure — most don’t feature 2FA like financial accounts, for example — and stolen goods and compromised accounts can easily be resold on grey market forums. It’s critical to stop fraudsters at the front door while enabling a good experience for genuine gamers.

2021 Early Attack Trends

Q1 Attacks

17%
Attack Rate

15 Million Daily
Attacks in the Busiest Weeks of Q1

Human vs Bots

3.4%
Human Fraud

96.6%
Bot Attacks

Over **2X Increase** in Human Attack Rate over Q4 2020

Mobile vs Desktop

32.6%
Mobile

67.4%
Desktop

75% Increase in Mobile Attack Rate over Q4 2020

2020: An Intense Year of Targeted Attacks

32.4%
Attack Rate on
All Transactions

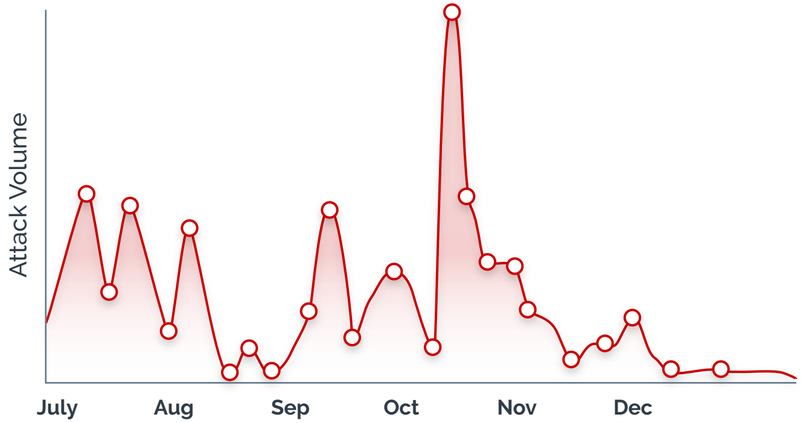
3.4B
Attacks in 2020

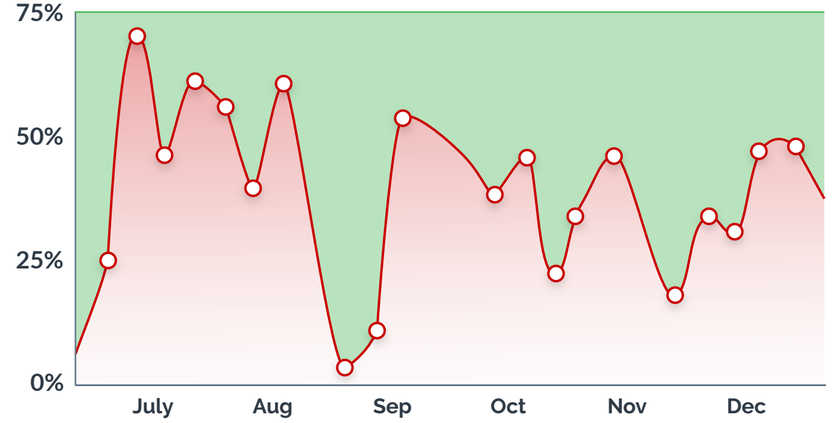
Key Target:
Logins

Looking back at 2020, it was a year of frequent and intense attacks targeting gaming, with periods of volatile spikes. At its peak in the 2nd half of 2020, up to 75% of traffic to online gaming platforms were attacks. These were largely driven by malicious bots.

Gaming platforms saw spikes in attacks in particular during holidays, and some days saw hundreds of millions of attacks. Major spikes in attacks were also seen during promotional giveaways, for example when free or discounted games were offered.

While attack levels have somewhat normalized a bit to begin 2021, gaming is still a highly targeted industry.





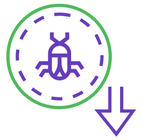
Top Trends at the Beginning of 2021

Increase in Human-Driven Fraud

Q1 saw human-based attacks coming online more than before. This highlights the continuing importance of fraud farms in disguising their identity amidst large volumes of legitimate players.

Rise in Malicious Mobile Traffic

Q1 2021 saw the highest level of fraud originated from mobile devices, following an increase in mobile gaming as a whole. Attacks from the mobile channel increased over 10 points from 19% in Q4 2020 to 32% Q1 2021.

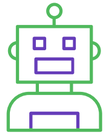


Drop in Attack Rate from Q4

2021 started like 2020 ended, with high attack levels. At its peak, the suspicious traffic rate was over 33%, but that has gone down to a more manageable 17% by the end of Q1.

A Diversification of Attack types

While 2020 was dominated by ATOs and login-based attacks, Q1 2021 saw a significant uptick in bots used to execute spam, in-game abuse, and gift card monetization.



The Rise of the Cyborgs

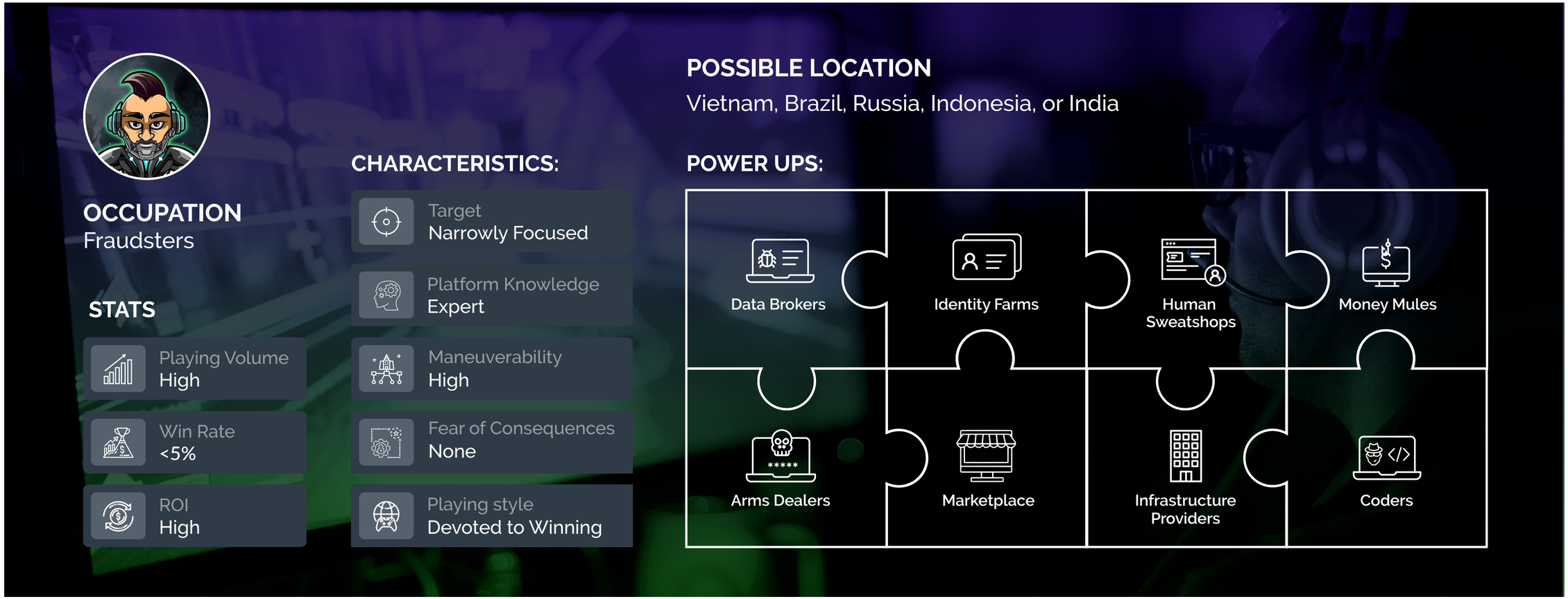
The increase in humans launching attacks speaks to the increasing relevance of so-called "cyborg" attacks -- with fraudsters deploying a mix of bots and fraud farms to successfully pull off attacks.

Fraudsters Disguised as Players

High surges of gaming traffic were goldmines for fraudsters. With more players to hide among and more players to target, it's no surprise we saw a rise in human fraud to facilitate in-game abuse in Q1.

What Does a Gaming Fraudsters Look Like?

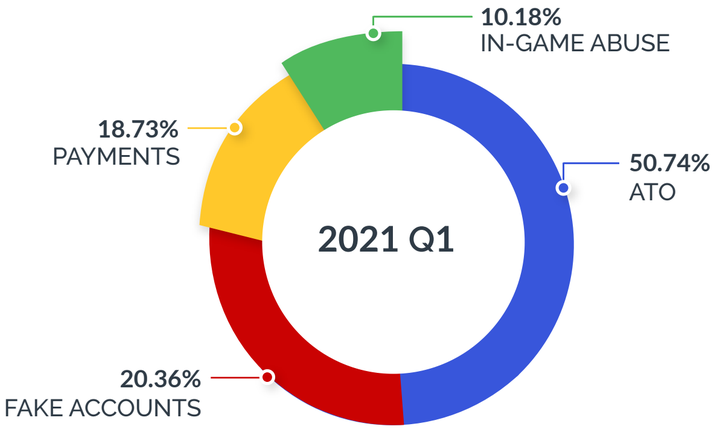
Fraudsters in the online gaming space are not your “typical” criminals. Many attackers ruthlessly target gaming platforms for their valuable in-game digital items and currency to resell on grey market forums. Gaming is also a popular “starting off” point for burgeoning fraudsters, since they use simple bots to launch attacks at scale. Gaming fraudsters work around the clock, leveraging an ecosystem of resources to hide amongst legitimate players. When they play, they play to win.



Diversifying their Attack Portfolio

Whereas ATOs were the primary attack vector at the end of 2020, fraudsters have started diversifying their attack methods to maximize their ROI. Let's take a deeper look at some of the top attack vectors.

Diversified Attack Vectors



There are a plenty of ways that bad actors can monetize attacks on gaming companies. Here are some of the most common:

Account Takeovers

Accessing genuine accounts to steal and resell players' hard-earned assets, or dormant accounts for in-game cheating.

In-Game Abuse

Using communication channels for phishing, spam, and malicious content.

Real-Money Trading

Auction house abuse, economy inflation and match-fixing.

Payments

Fraudsters targeting gift cards, credits, and player payment methods.

Fake New Accounts

Creating multiple new accounts to receive new account bonuses, spam legitimate players, or collude with other bad actors

Attack Vector 1 - Account Takeovers

While attackers have begun diversifying their attacks, in 2020 account takeovers were attack vector of choice for many fraudsters, comprising almost 90% of all attacks. At the height of Q4 2020, Arkose Labs recorded 70M daily ATO attacks on gaming platforms.

Fraudsters employ ATOs because there's a low barrier to entry. Mass credential spills have decreased costs and increased profits, making it an economical, efficient, and accurate form of attack. In fact, fraudsters can deploy large-scale and highly disruptive ATO attacks for as little as $15/day.

The real targets of interest for an ATO are the in-game items or funds on the account that can be resold on the gray market. Compromising accounts with valuable assets can earn attackers up to $3,000. Selling one high value account can cover an entire month's cost in a single day. As long as the score is worth the effort, ATOs will continue to be an attack pattern of choice.

Cost to Deploy Attacks
As little as $15/day

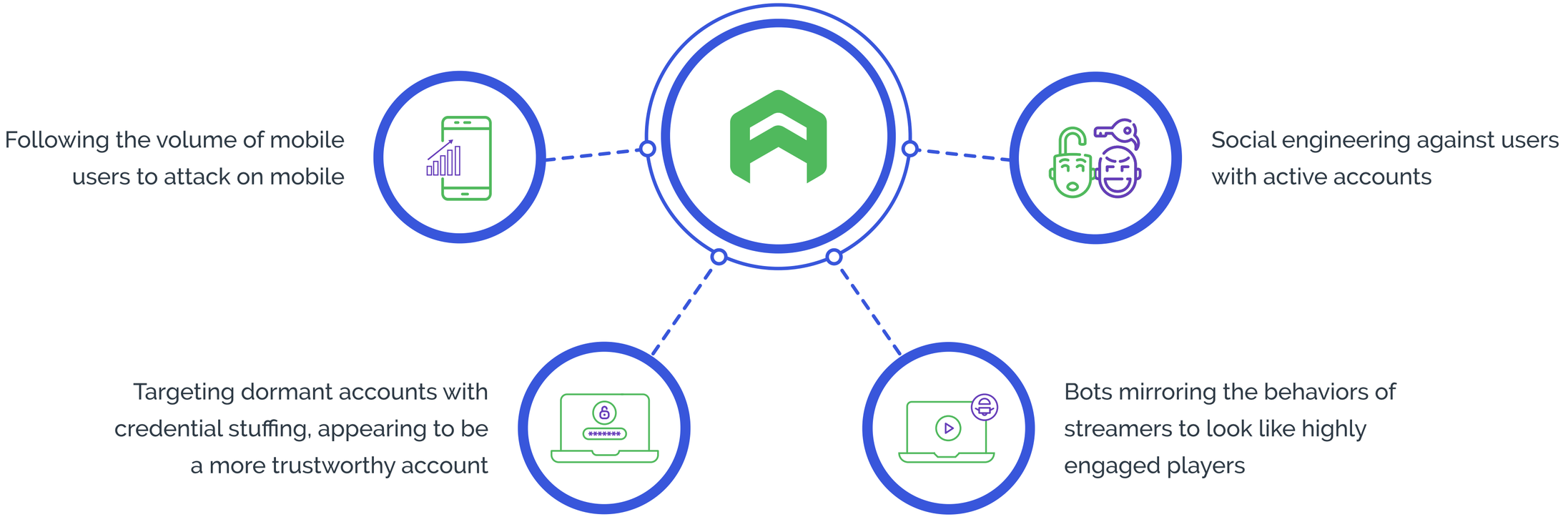
Compromised User Accounts

Up to $3,000 for valuable accounts

ATOs: Hiding in Plain Sight

2020 saw a shift from traditional botting to more targeted ATOs. With more players in the gaming arena, fraudsters are more motivated than ever to compromise good user accounts to sell their valuable inventory. Whereas in 2020 automation dominated attacks, smaller groups of more sophisticated attackers are devising a combination of human and bot strategies to target high value accounts.

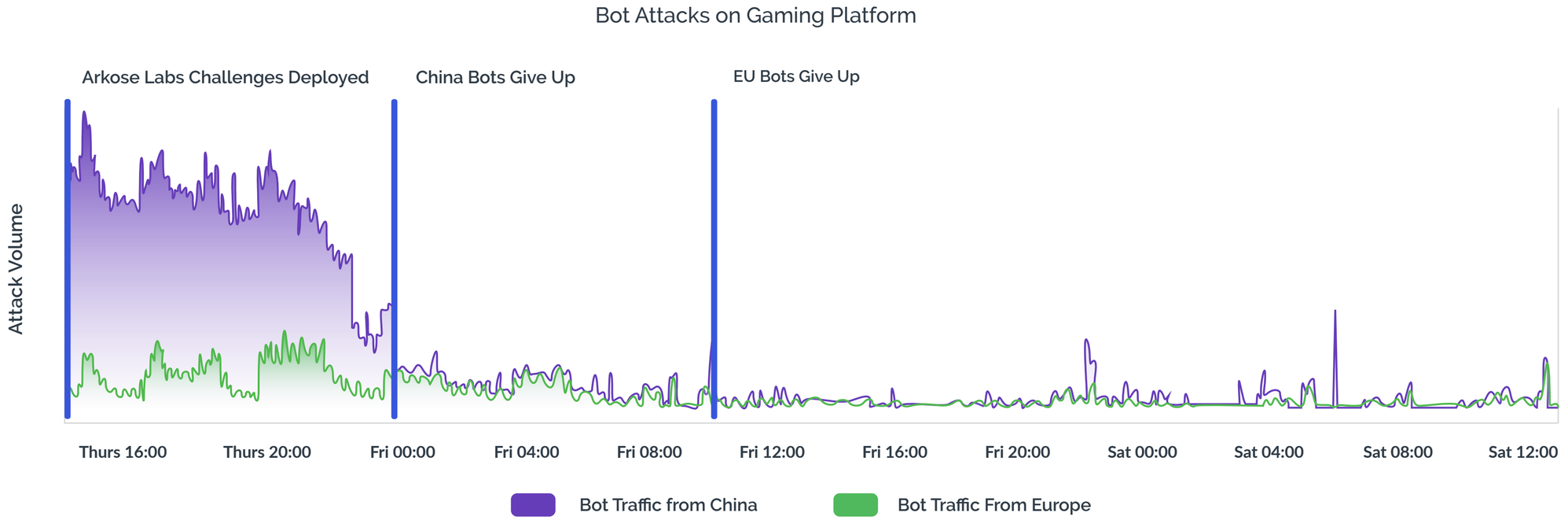
Recent tactics to help fraudsters expertly hide in plain sight include:



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.



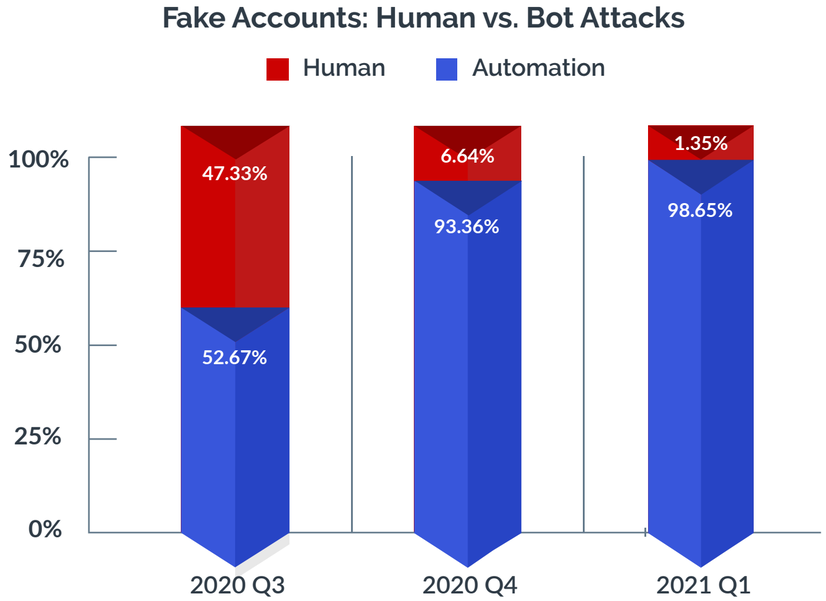
Attack Vector 2 - Fake Accounts

Whereas with account takeovers fraudsters can score big on one lucrative account, fake account creations are a volume play. These accounts can typically be resold for about $1 to $5 per 1,000. That means fraudsters need to create new accounts at massive scale to make money — and they deploy bots to do so.

That's a big reason why fraudsters leveraged more automation to target registrations on online gaming platforms than ever before. By training bots to mimic good user behaviours, they can easily hide while creating accounts at scale. The Arkose Labs network detected upwards of 2.1M daily attacks on registration at its peak during Q1.

Reselling Fake New Accounts

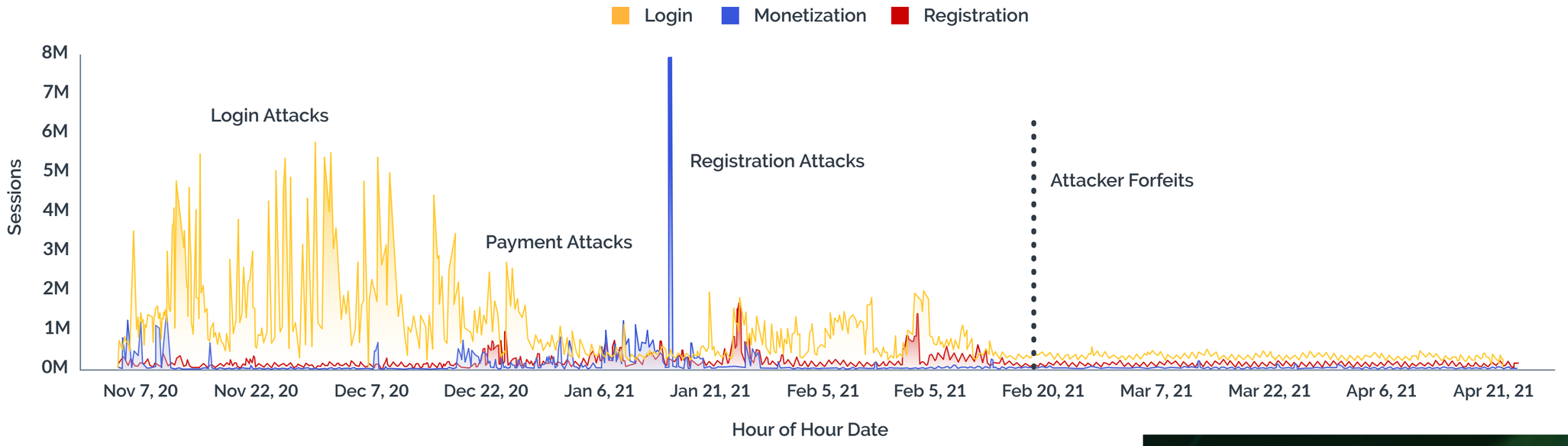
$1 to $5 per 1,000



Case Study: Targeted Attacker Gives Up

The ultimate win in any battle is when your opponent surrenders in defeat. One gaming platform scored a major win when their long-time attacker decided to throw in the towel.

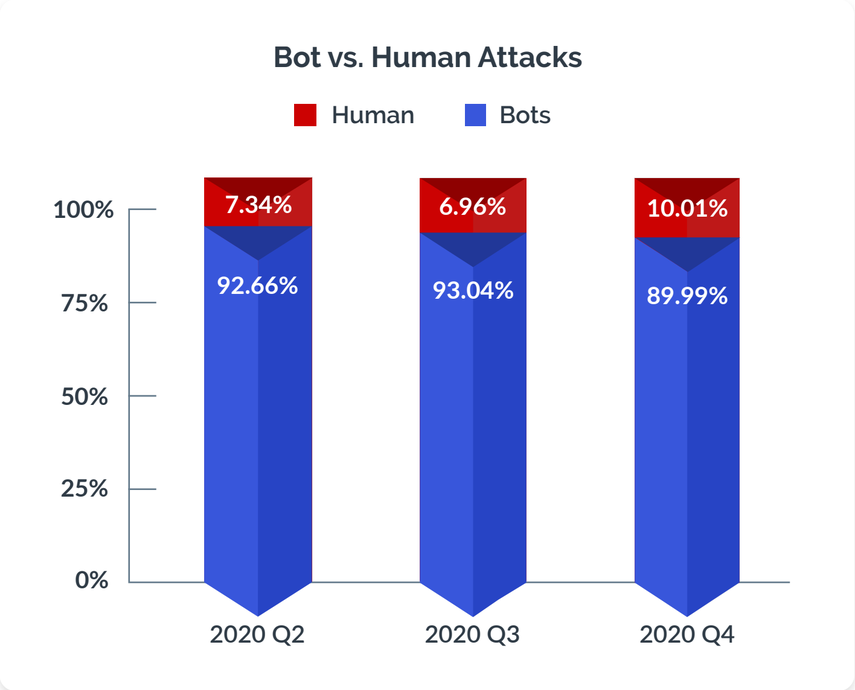
The platform was seeing recurring attacks on their network for quite some time. After deploying Arkose Labs, they noticed that attacks were coming from a single attacker. When met with resistance from Arkose Labs, the fraudster modified their tactics- trying registrations, logins, and payment vectors. The attacks continued to alternate between the two touch points trying to break through the barriers of the Arkose Labs platform. They even tried group joins to inflate the popularity of different groups within the platform. Despite the persistence of the fraudster, they were no match for the platform with Arkose Labs protecting their major customer touchpoints. In February 2021, attacks finally dropped off to nothing with no trace of the attacker.

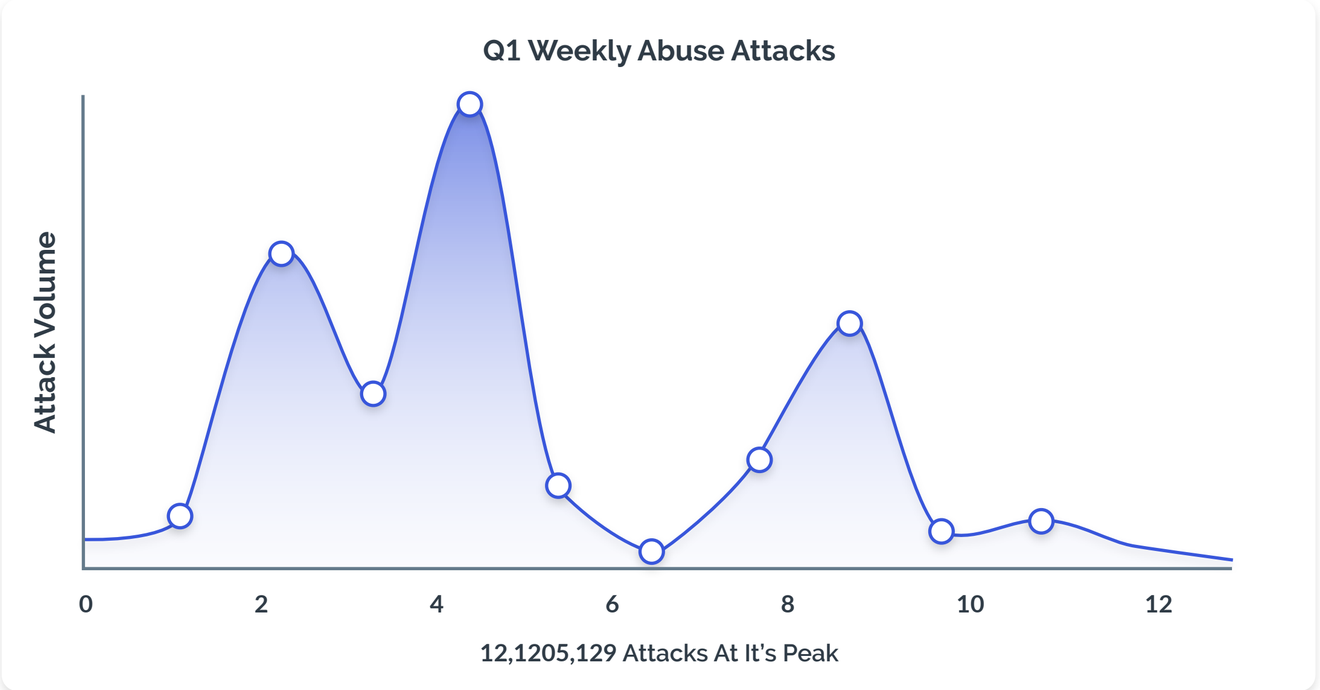


Attack Vector 3 - In-Game Abuse

The start of 2021 has shown the highest levels of in-game abuse in the last year. At its peak in early 2021, we saw upwards of 12M abuse attempts in one week.

As compared to ATO and fake accounts, fraudsters are more likely to leverage a combination of bots and fraud farms for in-game abuse, with 10% human fraud rate in Q1. In-game abuse requires more elaborate schemes to appear like a legitimate user, not just to the platform's defenses, but the players they target as their victims.





Fraudsters in Our Midst

Once inside the gaming environment, there are a multitude of vectors fraudsters employ to abuse the platform and lure players into their web.

Friendly Fraud

The gaming arena is a great place for young adults to learn how to code. However, many are easily tempted by the ability to cheat, level up, or make money in virtual game economies. Good users turned bad can be some of the hardest to spot.

Real Money Trading

Fraudsters know players seek to gather as much wealth and experience in a game as fast as possible. Rewards are sold to players on the gray market. Some nefarious guilds make money by selling paid services to other players to carry them through the highest difficulty content for exclusive achievements.

Social Engineering

Spikes in gaming over the last year are driven by gamers' desire for social connections. Finding love interests is no longer reserved for dating sites. In-game chats have become fertile for social engineering and catfishing as players bond over game play. With an increase in social activity on gaming platforms, there is greater return potential on phishing & scams.

Fake Reviews & Popularity Manipulation

Fraudsters often manipulate the integrity of gaming platforms. For platforms with user-generated games, they can artificially vote up certain ones to make them more popular. They can also upvote (or downvote) videos or any in-game reviews mechanism.

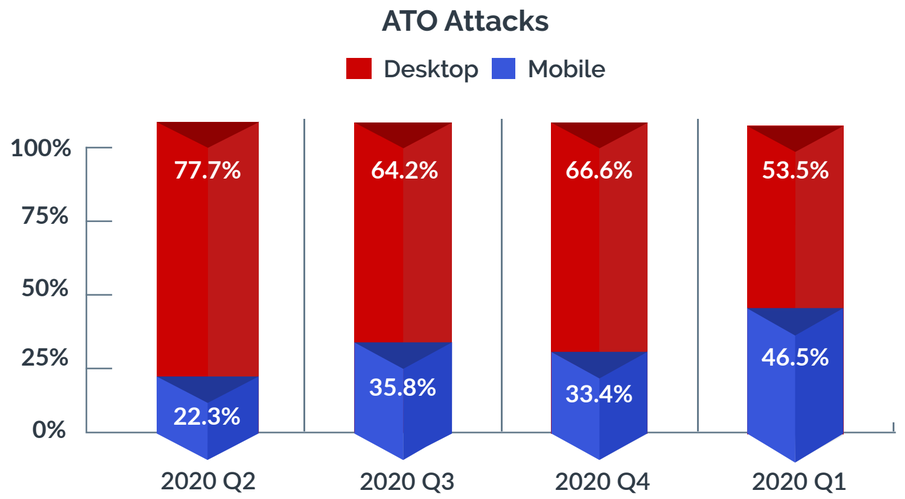
Gaming on the Go: The Rise in Mobile

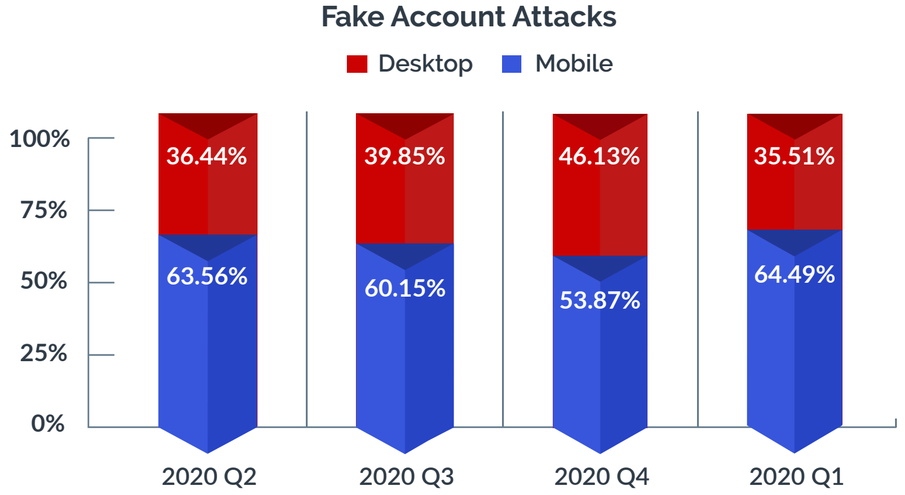
There has been a marked shift in the last year or two to mobile overall when it comes to gaming. Mobile has become a primary gaming device largely due to its easy accessibility and ability to play anywhere on the go, such as playing during work breaks or while traveling.

This in turn has led to an increase in fraud attacks originating from mobile devices. Fraudsters have a wide range of tools to emulate devices, and they can also purchase login details that come with the right device fingerprint from online dark web forums. As gaming becomes more mobile, expect fraudsters to increasingly utilize this channel to launch attacks.

Given these trends, it's probably not surprising to hear that in Q1, ATO attacks targeting gaming accounts were deployed almost equally to attacks launched from the desktop channel. This has been steadily increasing over the past year; in Q2 2020, the mobile attack rate on ATOs was only 22%.

When it comes to fake new account registrations, attacks coming from the mobile channel have remained consistently high, ranging between 50-65% of overall attacks over the past year.



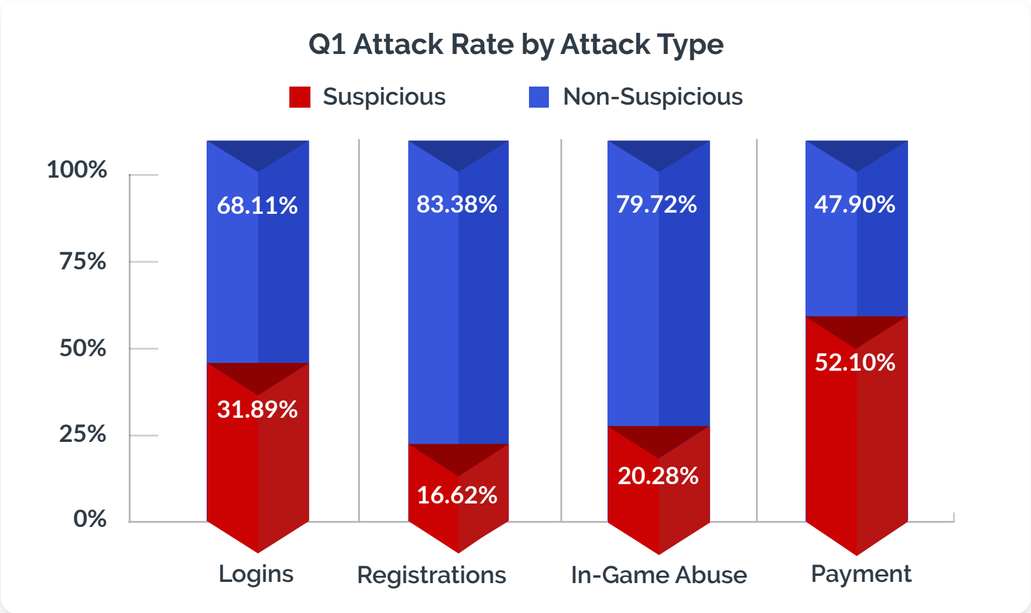


Attack Vector 4 - Payments

When you think of fraud, you traditionally think of bad actors trying to steal credit card information to purchase goods. In a world of gaming, bad actors can target gift cards and player credits, as well as payment methods to steal from good users.

In Q1 2021, fraudsters turned their attention to payment transactions more than ever before - with nearly 1 of every 5 attacks targeting payment information. Out of the key attack vectors, Q1 saw the highest attack rate on payment workstreams with over half of payment traffic consisting of attacks.

Gaming arenas are ripe for card testing fraud, testing stolen card information for accuracy. Because some gaming platforms have a multitude of microtransactions, it can be a good place for fraudsters to test stolen credit cards and use for bigger ticket items elsewhere. While card testing is an unavoidable part of digital commerce, it can cost platforms time & money in disputes and player dissatisfaction.



Conclusion: The Fight Against Fraud Never Stops

While attacks against gaming platforms have come down from their record highs during 2020, the industry still faces a massive challenge and remains one of the most attacked by fraudsters.

Gaming companies can't afford to let their guards down now. In addition to professional fraudsters, many "regular people" are committing fraud on gaming platforms as well, such as tech savvy teenagers engaging in hacks or manipulating in-game economies. And as the popularity of online gaming platforms continues to grow, coordinated attacks as well as so-called first party fraud will continue as well.

That's why it is more important than ever before that online gaming platforms — and indeed 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 defenses, and we can all help to 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