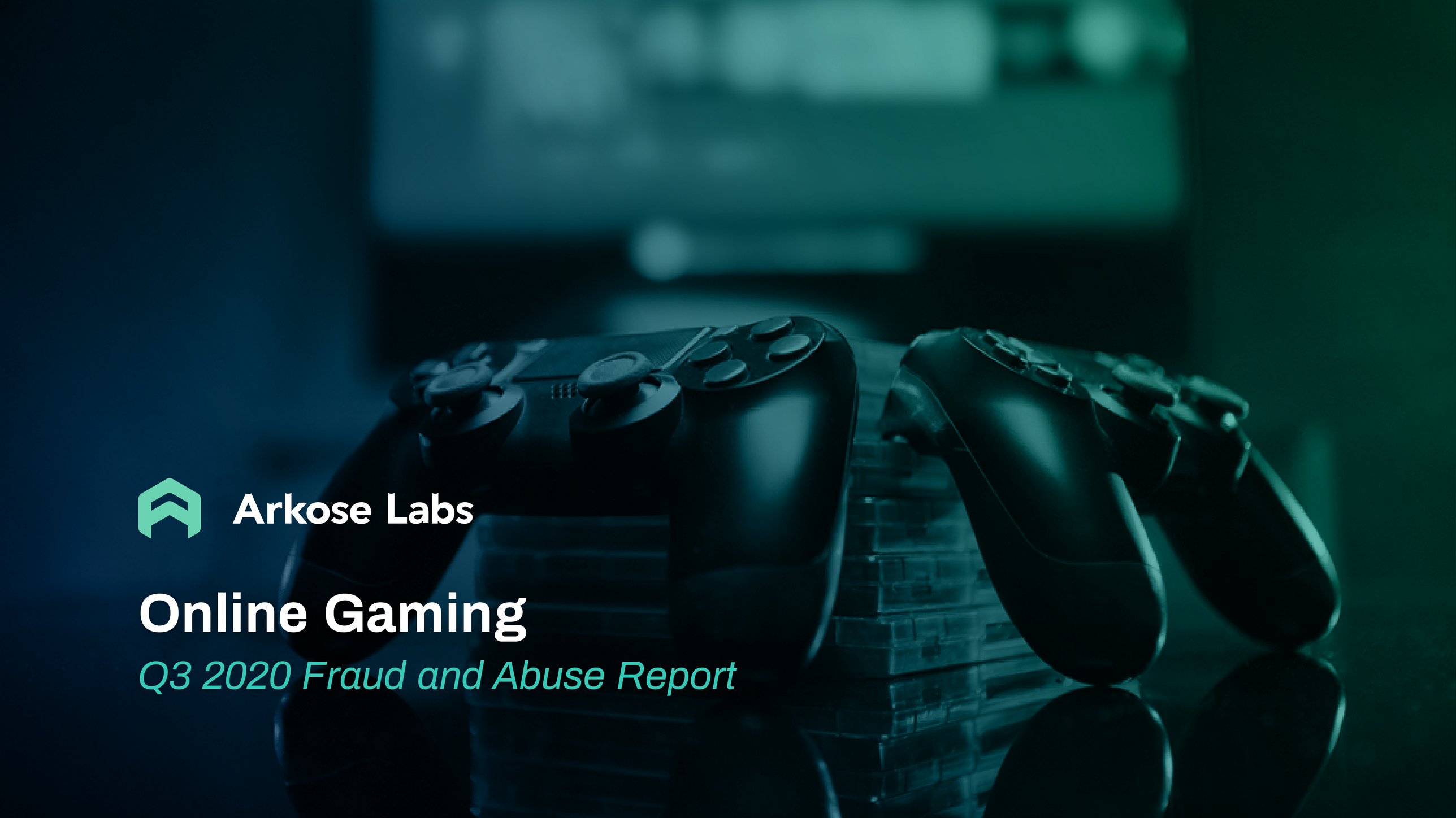


Arkose Labs

Online Gaming

Q3 2020 Fraud and Abuse Report

Introduction

Perhaps no industry has been affected by changing consumer habits brought upon by the pandemic-related lockdowns more than gaming. Quarantined citizens who had never picked up a gaming controller in their life flocked to gaming platforms as a way to pass the time with society shuttered. And regular gamers, with much more time at home on their hands, vastly increased their time spent playing. For online gaming platforms, every day became a weekend in terms of digital traffic.

So it comes as no surprise that, along with toilet paper, video game consoles were a popular panic buy during the lockdowns. As always, fraudsters follow the money, and with a massive spike in traffic and new customers, gaming was the most attacked industry during Q2 2020.

In fact, COVID-19 only exacerbated a trend of increasing traffic —and fraud — coming to the online gaming industry. Q2 2020 was in fact the fourth straight quarter in which traffic to gaming platforms rose. While automated attacks dominated previous quarters, the gaming industry saw a rise in human-centric attacks in Q2. This means that fraudsters are increasingly launching more hybrid and sophisticated attacks to monetize the increasing popularity in this sector.

It will be crucial for gaming companies to be able to handle this increase in traffic while being able to root out the fraudsters from legitimate customers.

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.

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

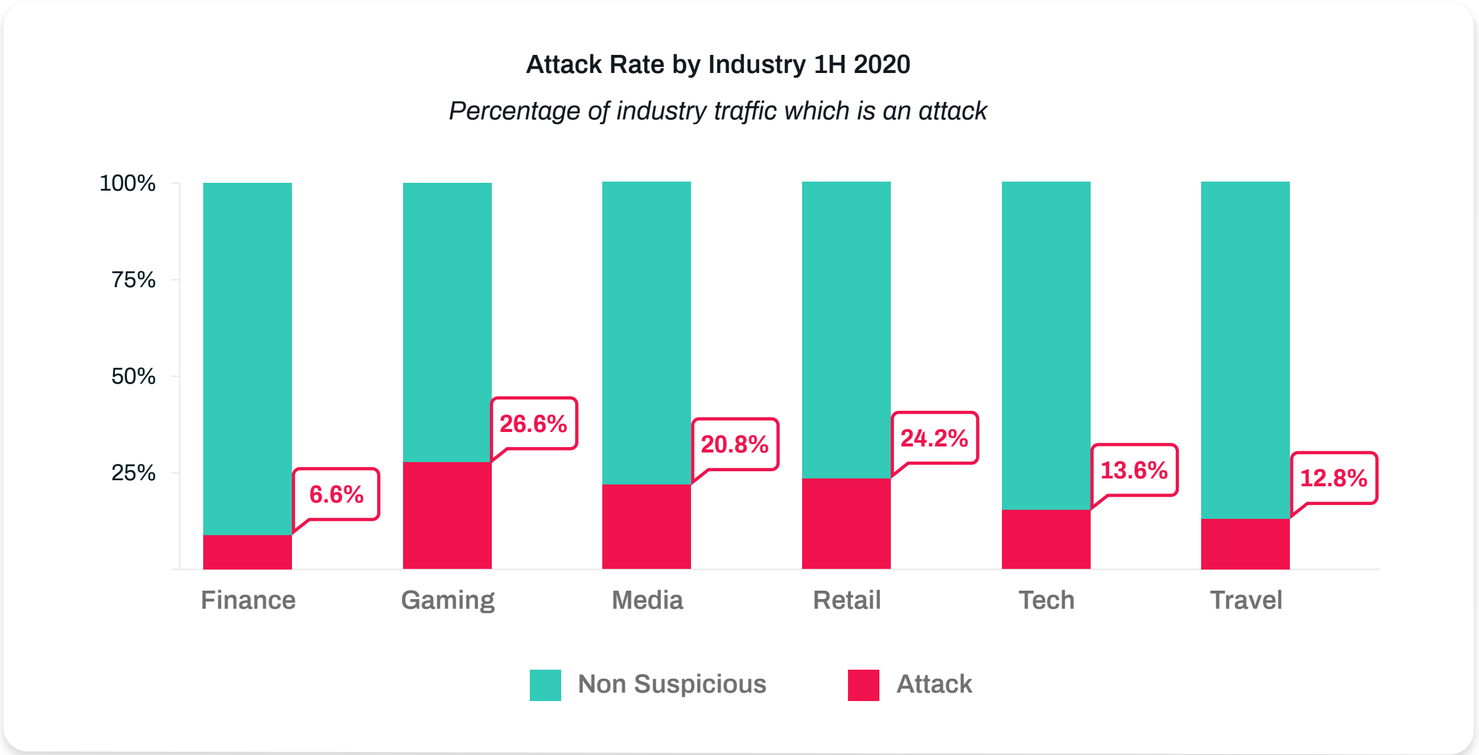
Most attacked
use case is logins

Gaming industry
sees most intense attack levels

65 attacks per second
for gaming industry

Gaming is a Top Targeted Industry 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.



Online Gaming Under Pressure During COVID-19

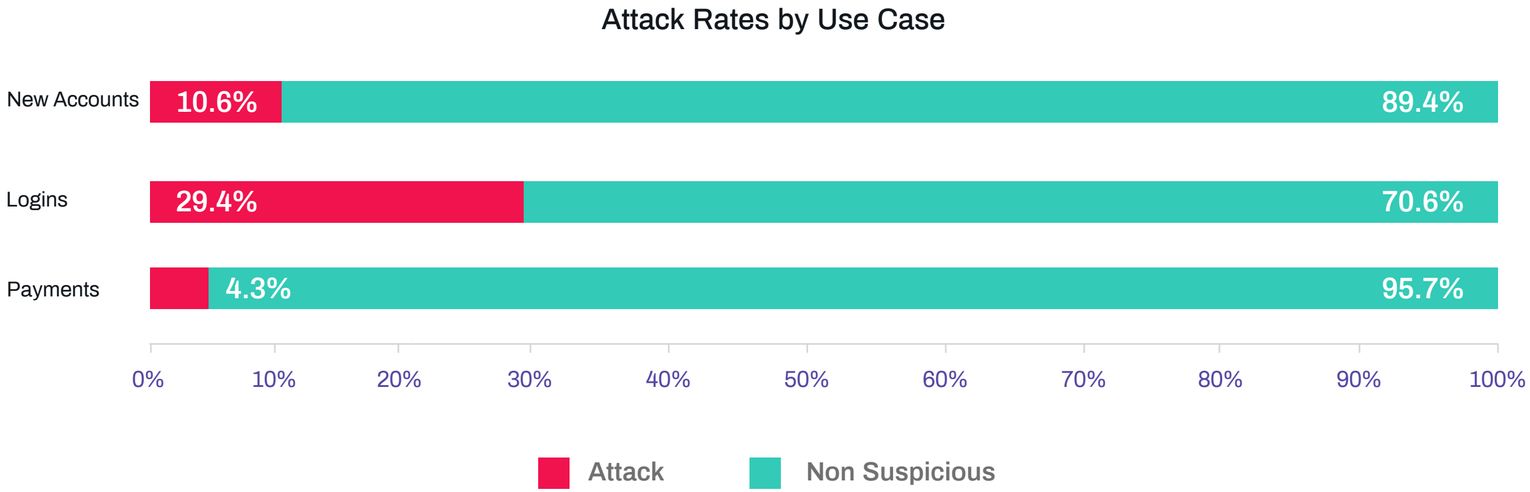
25%
attack rate

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.

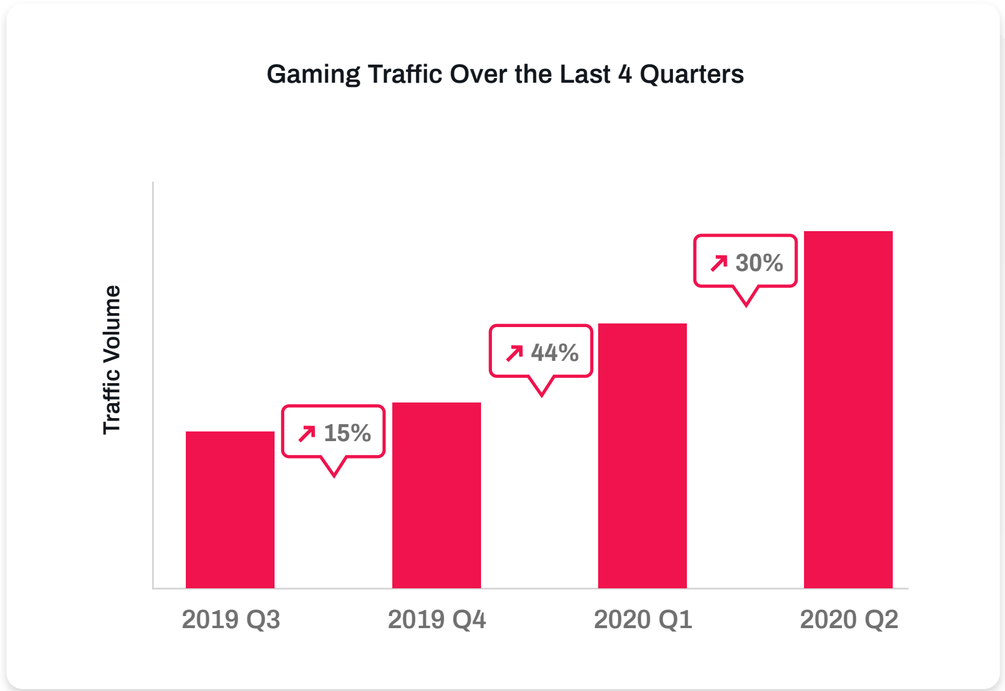
Q1 was dominated by automated attacks, as fraudsters leveraged tools to spin up attacks at speed as an immediate response to COVID-19. However, Q2 saw a shift to human-driven attacks, which accounted for 41% of gaming attacks. This returns the human attack mix to pre-lockdown levels, as 40% of attacks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

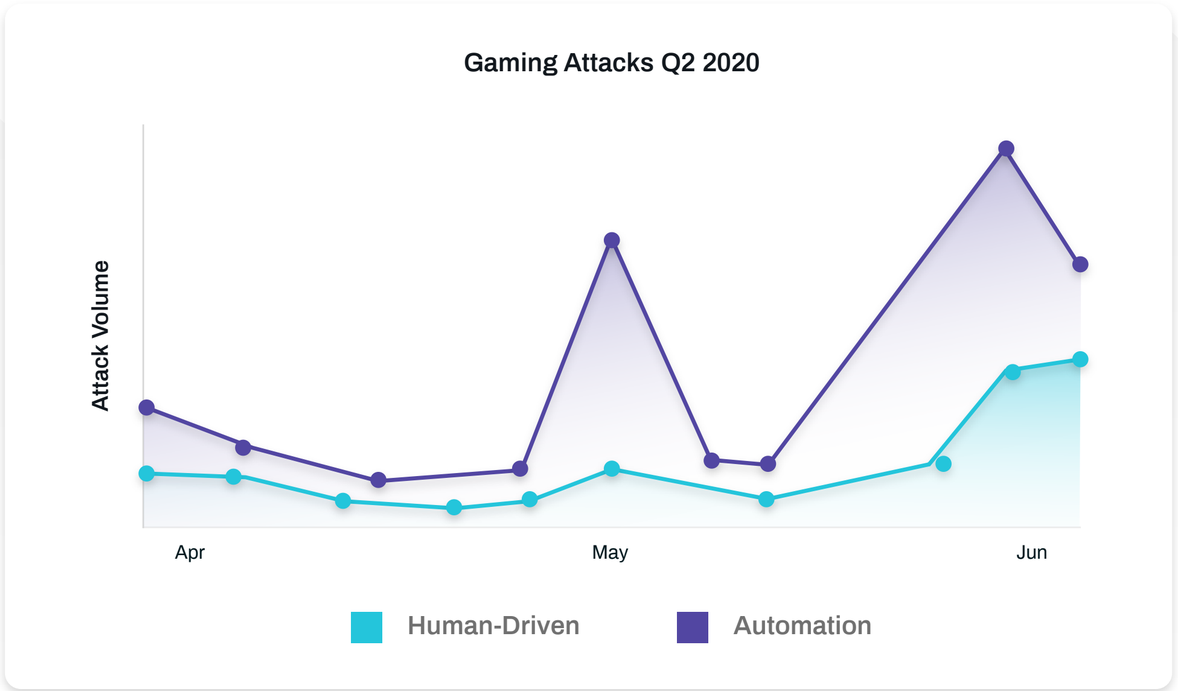


Gaming Traffic Explodes

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





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 one type of abusive activity which are used in-game 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.

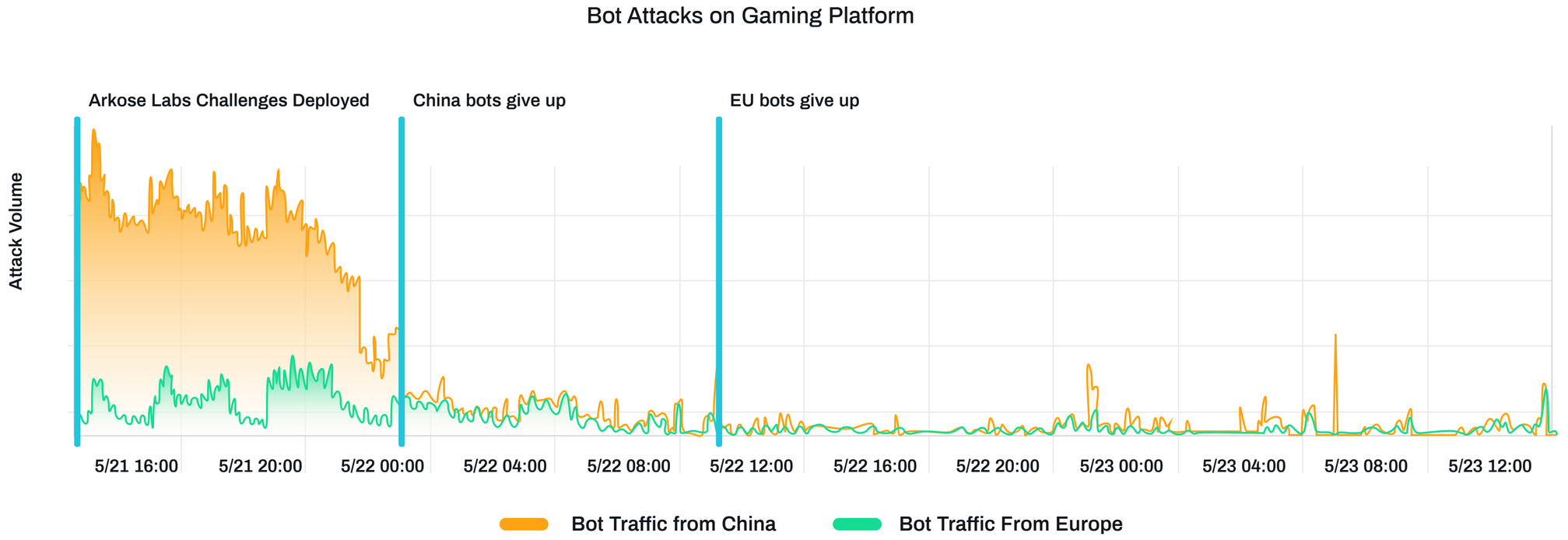
- Damages player sentiment
- Brand reputation suffers
- Harms user experience
- Takes away legitimate income selling assets
- Limits options for game designers

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

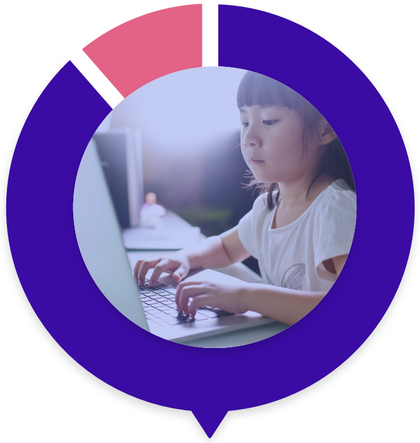
A major online gaming platform, with millions of global users, was facing large-scale credential stuffing attacks originating from China and Europe. Online support pages for customers experiencing account login issues were being hammered by bots looking to hack into legitimate accounts.

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.



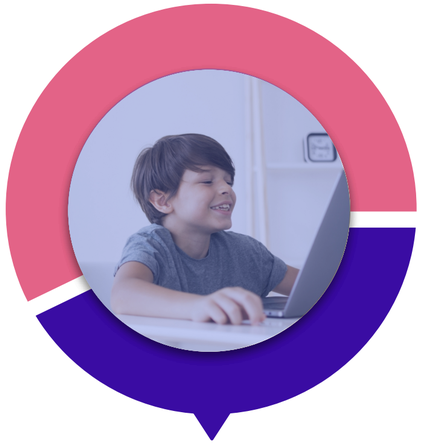
COVID-19 Lockdowns Accelerate Digital Adoption Among Kids

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 nteractions 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.



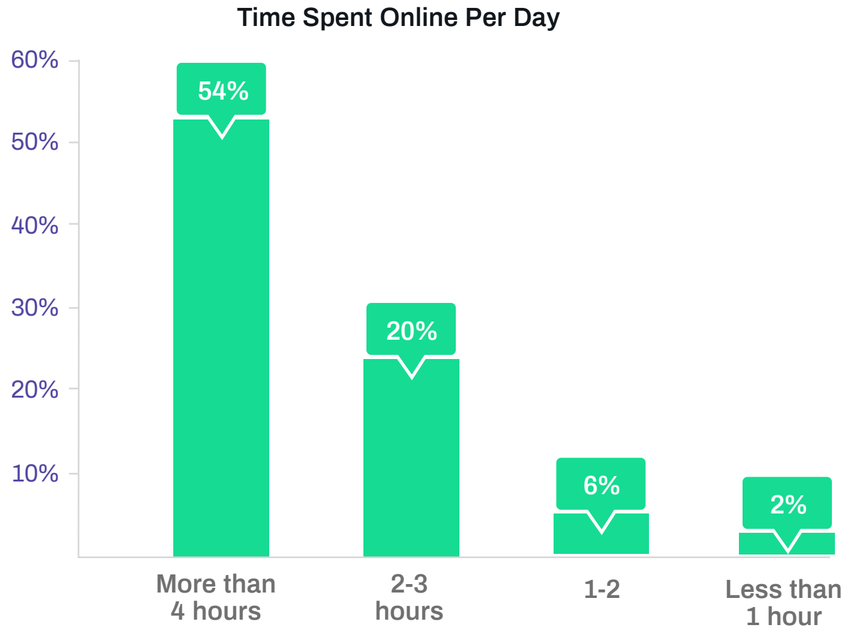
95%

of children spend more time online due to COVID-19



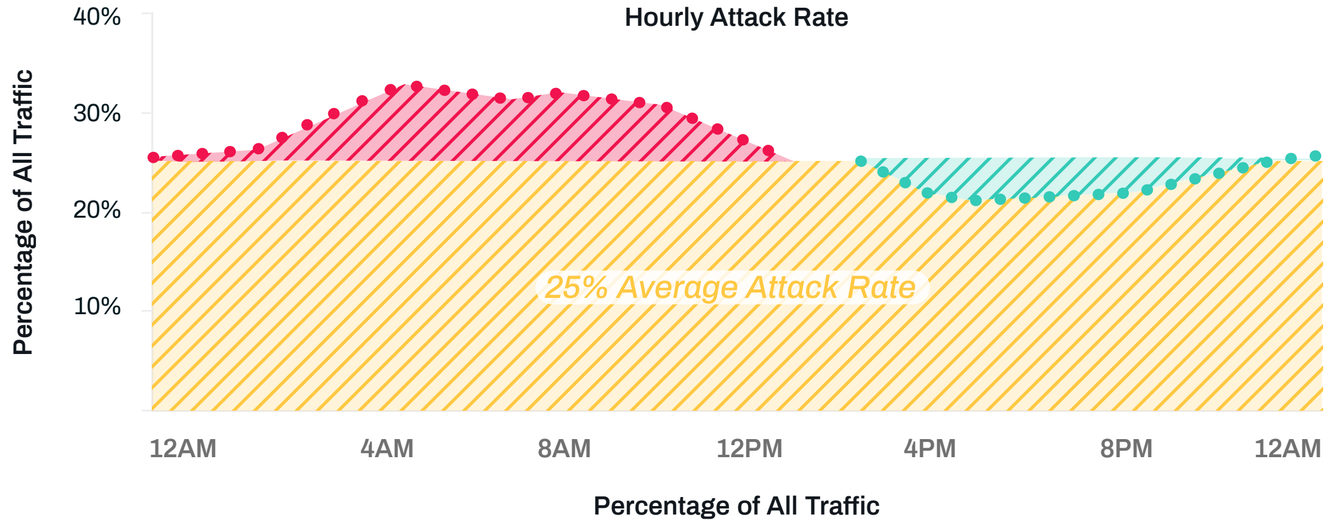
44%

of children careful sharing information online



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

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 on Q1, when sweatshops 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 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.

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.

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

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.

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