Arkose Labs

2022 STATE OF FRAUD & ACCOUNT SECURITY

Insights from the Arkose Labs Global Network

Table of Contents

The 2022 State of Fraud and Account Security Report is based on actual user sessions and attack patterns across a global network of websites & apps using the Arkose Labs Fraud Deterrence Platform in 2021. These sessions, spanning account registrations, logins and payments from financial services, e-commerce, travel, social media, gaming and entertainment, were analyzed in real-time to provide insights into the evolving fraud and risk landscape.

Introduction

A common phrase heard in the past few years is “data is the new oil.” The digital world now encompasses so much of our everyday lives, and data is the valuable commodity that fuels it. It’s not just commerce that operates largely in the digital realm, but also work, socializing, education and much more. In fact, the concept known as the metaverse could become an $800 billion market by 2024, according to Bloomberg Intelligence.

This will lead to an exponentially larger attack surface for fraudsters to target. Rather than just PCs and mobile devices, attackers can compromise smart appliances, connected automobiles and virtual reality devices. So it’s no surprise that fraud attacks are increasing dramatically. But they are increasing not only in volume, but also sophistication. Bots become more nuanced and advanced by the day; able to mimic good users with increasing accuracy and bypass defenses. Automation is the key for attackers to be successful in their endeavors. It allows them to attack at such scale and so inexpensively that only a small percentage of their efforts need to be successful to turn a profit. Meanwhile, businesses continue to pour time and money into cybersecurity and anti-fraud defenses only to fight a losing battle.

In this new world, businesses and all digital platforms need to upgrade and advance their fraud and security defense tactics in 2022. What worked in the past is no longer viable, and they will need to adapt to ever-evolving attacks that target many touchpoints. In this report, we will discuss some of the trends from the last year and must-haves for 2022 based on insight from billions of sessions across the Arkose Labs network. The task of fighting fraud is difficult, but together we can make the digital world now and in the future safe for all.

Kevin Gosschalk

Founder and CEO

Digital platforms need to upgrade and advance their fraud and security defense strategies in 2022. What worked in the past is no longer viable, and they will need to adapt to ever-evolving attacks that target user touchpoints.

https://www.marketwatch.com/story/what-is-the-metaverse-and-how-much-will-it-be-worth-depends-on-whom-you-ask-11637781312

21%
attack rate

1 in 4
new account registrations are fake

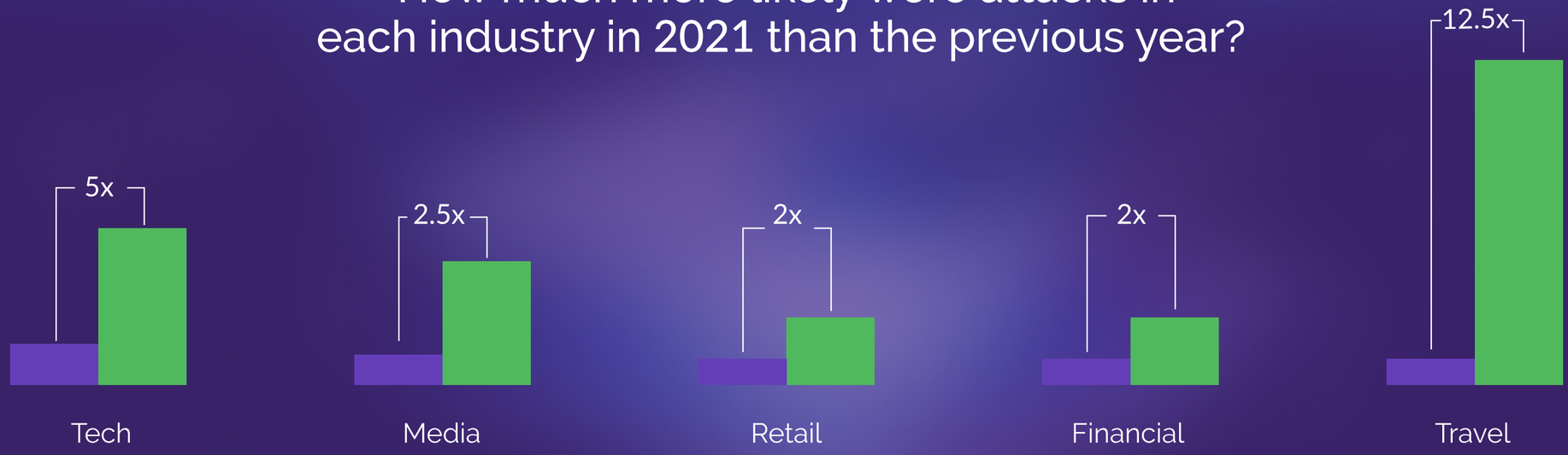
80% of login attacks are credential stuffing

86% of all attacks are bots vs human

16%
increase in mobile traffic

5 in 6
industries saw increase in attack rates

How much more likely were attacks in each industry in 2021 than the previous year?



Top 6 Attack Trends of 2021

The Year of Account Security

2021 was a year when account security became paramount. Attackers targeted both login and registration points at scale due to the great monetization potential.

85% increase
in login & registration attacks

Attackers Follow User Engagement

2021 saw a significant uptick in the rate of attacks across all industries. The vast majority saw a 400% increase in attacks, with attacks on travel seeing a major resurgence.

User actions in 2021 were
4x more likely
to be attacked over 2020

Volatile Attacks Are the New Norm

Attacks are more volatile than ever, and businesses need to be adaptable to mitigate damages fast. High velocity attacks can unexpectedly overwhelm fraud and security teams and even cause major strain on infrastructure.

A single attack can consume
80% of traffic

Intelligent Bot Revolution

Bots are increasingly sophisticated, able to mimic human behavior with a high degree of accuracy. As such, businesses are dealing with more complex attacks that require more sophisticated analysis to detect anomalies.

3x more complexity in
detecting bots

Welcome to the Metaverse

The beginnings of a concept known as the "metaverse" means a new attack vector for bad guys. Early insights from our global network show scams, microtransaction abuse, and unfair play to be top threats in a metaverse world.

Metaverse companies experience **80%** more bot attacks than other businesses

Asia Leads as Top Attacking Region

While attacks out of Russia were more common in years prior, attackers out of Asia came out to win in 2021. Leveraging an ecosystem of tools and low-cost resources, China took aim at the tech industry to abuse free trials for crypto mining.

40% of attacks originated from Asia, with China as the top attacking country

2021: The Year of Account Security

In many ways, our digital identities are just as important and valuable as our physical identities. Nearly all aspects of our lives are conducted online, and each platform we use for shopping, entertaining, socializing, working and more, is associated with a digital account; indeed, these have become a stand-in for our identities on the internet. The average person now has more than 100 passwords, according to some studies.

These digital accounts, if they are compromised, give attackers access to then commit a wide range of fraud and abuse beyond just stealing personal information. With nearly 1,300 data breaches recorded through September 2021, it is no surprise that digital accounts are a huge target for attackers. Across the Arkose Labs Network, attacks targeting either the login or registration point increased by 85% year over year.

Once attackers have compromised an existing account, they can monetize it in a number of ways, such as stealing financial information, reselling the credentials, redeeming accrued loyalty points and more. Fake new accounts are used for attacks such as inventory hoarding, content scraping, and sending spam and phishing messages.

1 in 5
logins is an ATO attempt

Registration attacks were
2.5x more likely
in 2021

85%
increase in attacks on logins and sign-ups

https://www.techradar.com/news/most-people-have-25-more-passwords-than-at-the-start-of-the-pandemic
https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021

Fraud Follows Consumer Behavior Across Industries

There's a direct relationship between fraud and consumer behavior. As seen in past years, there was no doubt that attacks and monetization of digital accounts would continue to shift with environmental influences and wherever businesses saw growth. As expected, businesses that hit high-growth periods in 2021, saw an increase in attacks.

Gaming saw sky-high attacks in 2020, but leveled-off in 2021, which led to attacks dispersing across other industries. Online media and entertainment continued to grow in popularity, bringing more in-platform spam & scam attacks. Attackers flocked to the travel industry to take advantage of scraping and inventory hoarding opportunities as the world shifted more toward post-pandemic normalcy.

Top Surprises of 2021

Attack Rate Increased Fourfold
Increased monetization potential of digital accounts increased the probability of user actions being attacked by 4x

Bots Followed Travelers En Masse
Attackers preyed on the travel resurgence, with scraping attacks compromising a massive 45% of traffic on travel sites.

Fraud Deterred in Gaming
With learnings implemented from unprecedented attacks in 2020, gaming attacks declined 2x faster than user engagement

Fake Accounts Are Increasingly Lucrative
Fake account attacks increased by over 300% in 2021, driven by phishing, scams, and free trial abuse

Top Trends Across the Industries

With the exception of gaming, every industry saw massive growth in attack rates as consumers and businesses alike embraced digital transformation. Each industry was targeted in different ways and by varying attack patterns. Throughout the highs and lows of 2021, businesses experienced spikes in new and reemerging attack types based on the rapidly changing environment.

Travel

- 45% attack rate amidst post-pandemic travel resurgence
- 95% bot-driven attacks
- Top threats: scraping & inventory denial

Tech

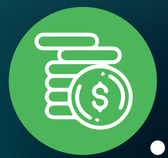
- 5x attack rate over 2020
- #1 target of attackers from China
- Top threat: creating fake accounts to abuse free trial benefits

Media & Entertainment

- 2.5x attack rate over 2020
- Most attacked platforms: social media & dating sites
- Top threat: 50% increase in fake accounts, driven by spam and abuse

Retail

- 1 in 4 transactions was an attack
- Growth in attacks outpaced growth in good traffic by nearly 3x
- 1 in 2 attacks are human-driven



Finance & Fintech

- 2x attack rate over 2020
- 70% increase in login attacks, driven by account takeovers
- Top threat: credential stuffing

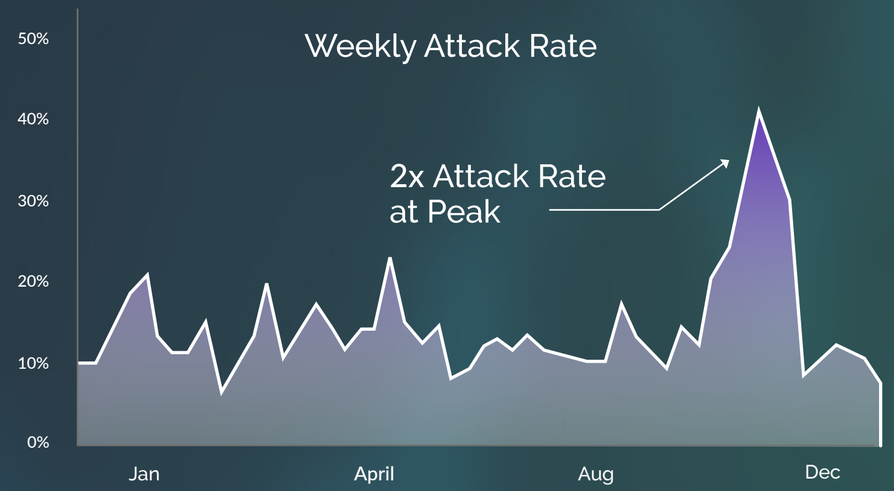
Gaming

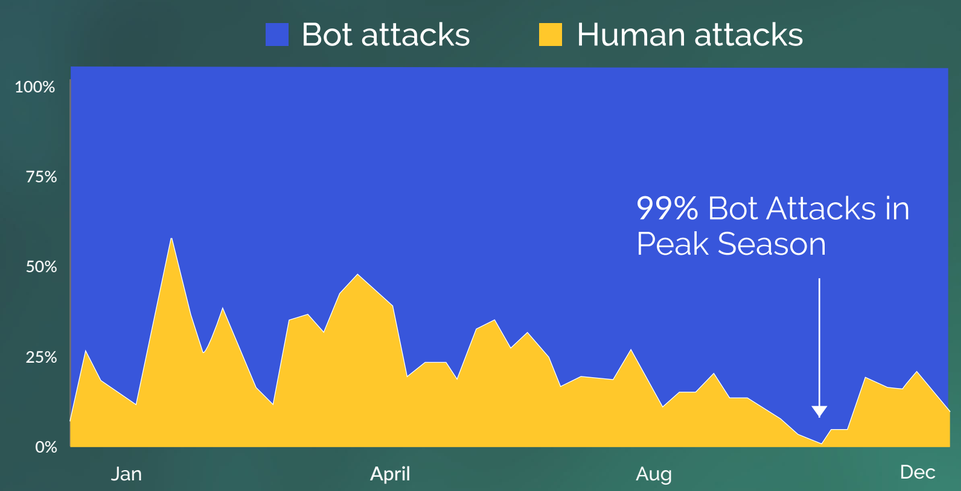
- 3x less likely to be attacked vs. 2020
- 2 of 3 attacks target user logins
- Top threats: credential stuffing, fake accounts, hybrid bot-human attacks

Volatile Attacks Are the New Norm

With an ever-increasing arsenal of tools at their disposal to attack at volume, bad actors are launching more volatile attacks than ever before. Attacks can be low and slow, trying to go undetected, or alternatively aiming to overwhelm defenses and make money from sheer volume. For example, November was the most dangerous month of 2021, with attackers capitalizing on the commerce period increasingly known as Black November. Retailers weren't the only target, though. Financial services saw 3x the normal attack rate over the holiday season and 1 in 5 social media accounts were malicious. During peak periods, it's not uncommon for the attack rate to more than double, as attackers use bots to attack at scale.

Peak attack periods can be different for every industry, and include special events and major launches. Digital businesses must be prepared for a multitude of of sophisticated attacks using a mix of bots and human fraud farms. Every major revenue opportunity needs to include a plan for how to protect from an increase in attacks.



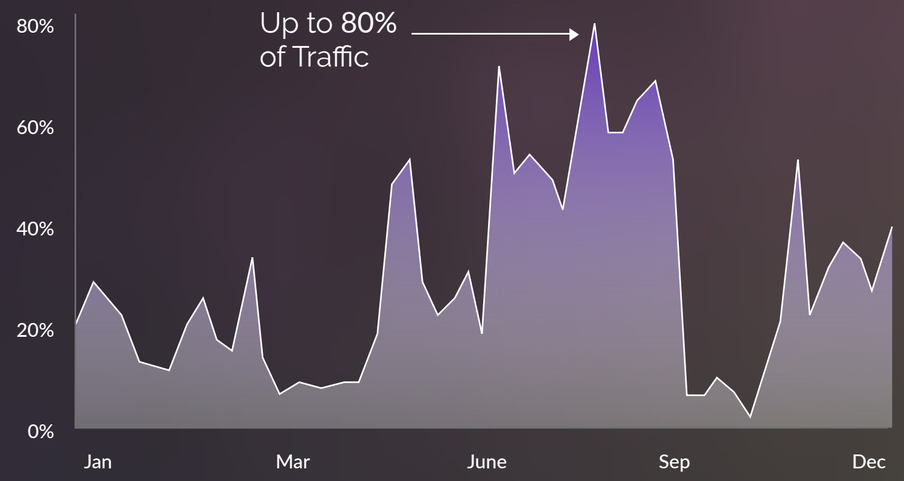


Businesses Must Prepare for Abnormal Patterns

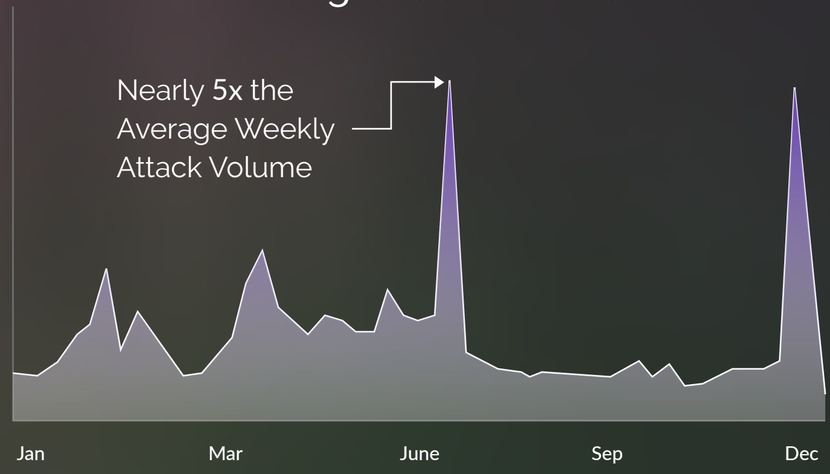
More volatile attacks mean that the “typical” patterns fraud and security teams look for in digital traffic can no longer be relied upon. Old models are becoming obsolete as attackers evolve their tactics and strategies. This is especially true for credential stuffing attacks, which can cause extreme spikes in volatility – some of the most intense attacks detected measured upwards of 76 million credential stuffing attempts per week.

One global tech company that is protected by Arkose Labs saw a sudden and unexpected spike in credential stuffing attacks, that accounted for nearly 80% of its overall digital traffic. Another client, a major travel site, was inundated with scraping bots, with 35 million malicious bots hitting their site per day during the attack. Arkose Labs' team worked closely with the businesses to contain and remediate these attacks, to protect their websites and apps.

Tech Company Weekly Attack Rate



Travel Industry Weekly Credential Stuffing Attack Volume



The Intelligent Bot Revolution

Bots are indispensable in carrying out fraud and cybercrime; in fact, 86% of all attacks in 2021 was an automated attack. Attackers increased their usage of bots last year across all industries, despite businesses' increasing investments in bot management. Bots allow attackers to launch thousands of attacks in a matter of seconds and achieve far greater profit with quantity over quality. Bots are also increasing in sophistication at a fast pace; they are easy to deploy and relatively inexpensive for the attacker to acquire.

We already need to analyze **3x more values on average to detect today's bots,** compared to 18 months prior. This complexity is expected to accelerate over the next few years. Intelligent bots are beginning to carry out complex attack orchestration, wherein multiple scripts are used to perform different functions of an attack. This includes tapping into stolen and synthetic credential providers, device and IP spoofing, CAPTCHA solving services, and more. We expect hybrid attacks, which seamlessly link up attack scripts and organized human fraud farm operations to become the norm over the next few years.

Automated Attack & Evasion Orchestration

What to Expect from Intelligent Bots:

- Sophisticated evasion techniques
- Emulation of human behavior & responses
- Complex orchestration of attacks
- Hybrid human-bot “cyborg” attacks
- New monetization across digital front-end
- Spoofing & emulation erodes trust in signals

Into the Metaverse

2021 saw the emergence of the metaverse. Many brands are investing in our virtual future - building AR/VR-driven worlds where people can socialize, engage in commerce, play games, collaborate, and more. While this concept offers increasing consumer engagement and profit potential, it also creates another large attack vector that bad actors can target. Arkose Labs is fortunate to work with many metaverse pioneers, providing early insight into what attacks targeting virtual worlds look like.

As digital identities become more and more of an extension of our physical selves, compromised virtual accounts can feel more personal than ever and have a greater impact on brand sentiment. Virtual environments are prime targets for "Master Fraudsters" to carry out malicious activity including microtransaction fraud, spam, scams, and unfair competition. These are the more persistent attackers who script together multiple tools, use fraud farms, and are willing to invest more capital to bypass defenses. With highly persistent attackers and high stakes, companies investing in the metaverse must put a premium value on trust & safety at login, registration, and in-platform actions to protect digital identities in their virtual worlds.

Emerging Trends in the Metaverse

Metaverse companies experience **80%** more bot attacks & **40%** more human attacks than other businesses

Metaverse companies are more likely to be targeted by highly advanced attackers called **"Master Fraudsters"**

Metaverse companies are a prime target for:

Microtransaction Fraud

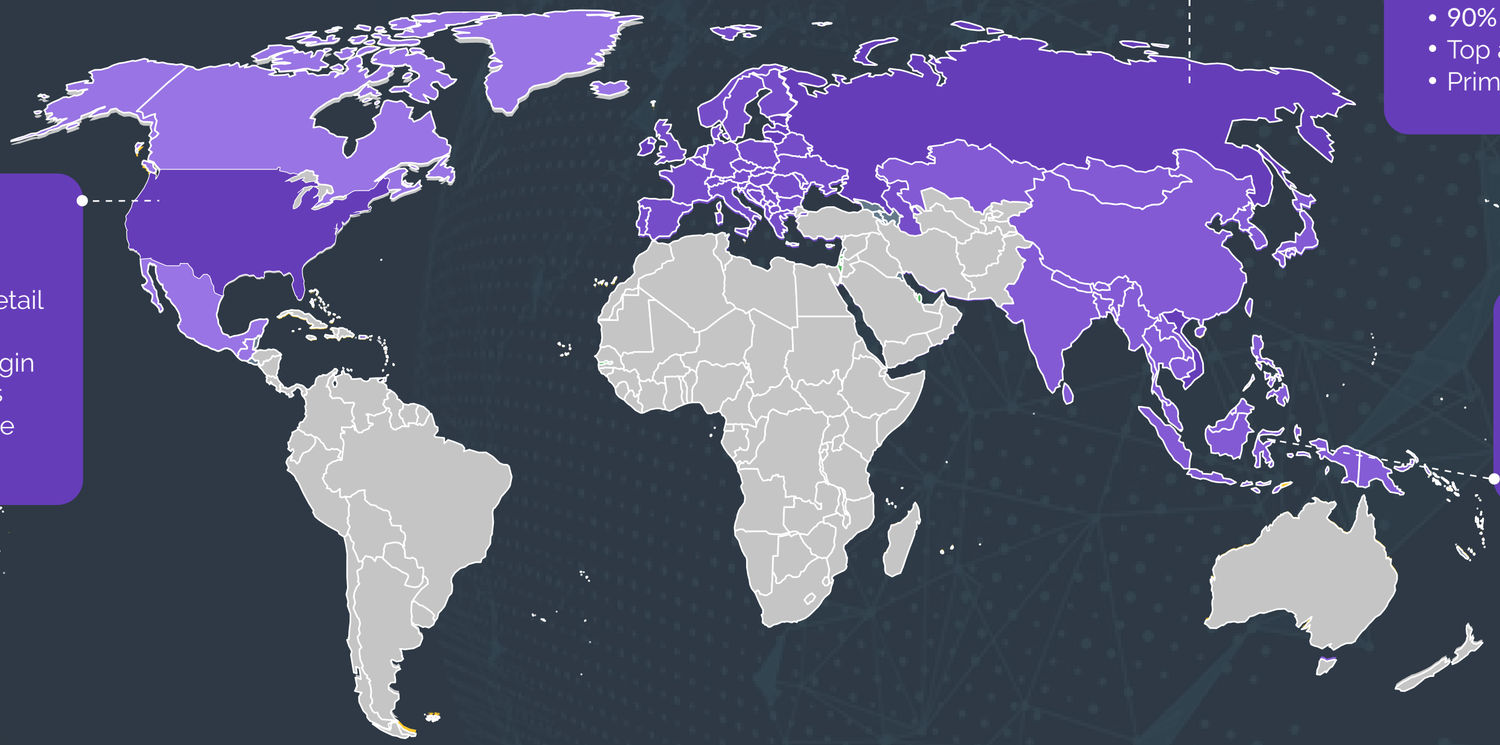
Disrupting fair commerce

Scams

Spam

Regional Attack Trends Driven by Socio-Economic Factors

Attack patterns differ by region, as disparities in wages, cost of labor, and comparative currency values dramatically shift, incentive levels among would-be fraudsters across the globe. For example, attackers from a country whose currency has been devalued will be more motivated by lower yield targets than those from stronger economies. Despite the volatility of cryptocurrencies, these remain a very high value target across the globe, and have been a particular focus for attackers from Asia. Here's how economic drivers contributed to attacks seen across industries in 2021.



EUROPE

- 55% of attacks are on registration
- 90% of attacks were bot driven
- Top attackers: Ireland and Russia
- Primary Targets: social media

NORTH AMERICA

- 30% of attacks targeted retail & travel
- 2/3 of attacks targeted login & registration touchpoints
- 55% on finance attacks are from North America

ASIA PACIFIC

- 1 in 2 of attacks in Asia were from China
- 2/3 registration attacks, driven by free trial abuse & cryptomining
- Primary targets: Tech and gaming

Key Fraud Prevention Strategies for 2022

To keep up with evolving attack patterns, here are 4 must-haves in every digital businesses' fraud prevention strategy in 2022

Advanced Bot Detection

Bots are more sophisticated than ever, able to mimic human behavior online and evade known defenses. It will be imperative for businesses to deploy nuanced strategies powered by machine learning to detect the subtle signs of advanced bot attacks.

Multi-Layered User Behavior Analysis

Since the line between what looks like good and suspicious traffic has blurred, it creates a large "gray area" of traffic that is neither obviously good or bad. Businesses need advanced behavioral detection on top of device and network intelligence to uncover bad actors from good users.

Powerful Challenge Strategy

Off-the-shelf bot programs that solve basic CAPTCHA in seconds are cheap and easy to deploy. Attackers also deploy human fraud farms to bypass anti-bot challenges. Businesses need a challenge strategy that stops even advanced bots and frustrates human CAPTCHA solvers, while also not adding friction to good users.

Actionable Insights to Work Smarter

Manual reviews can no longer scale with growth and high-volume attacks. Businesses need intelligent detection they can rely on to provide actionable insights and do the heavy lifting of assessing risk. The right mix of insights and programmatic attack response can free up fraud, security and identity teams to focus on more value-added tasks.

Advanced Bot Detection

With the intelligent bot revolution knocking on our doors, digital businesses need to evolve their bot detection and defense strategy for 2022.

Despite our best efforts, attackers leveraging automation are having more success than ever. Using tactics such as IP & fingerprint spoofing and headless browsers, today's more sophisticated bots rely on complex signatures to look like a legitimate user and sneak past traditional bot defenses. With the increasing number of data points that need to be collected, reviewed, and correlated, fraud and security teams need multi-layered detection and real time analysis that uncovers faults in the bot's story across network, device, and behavioral signals.

Best Practices for 2022:

Invest in IP Intelligence: More robust IP intelligence forces attackers to spend more on Proxy IPs, thus driving up their cost. With a diminished ROI, attackers abandon their sabotaging attempts.

Advanced Spoofing Detection: Having sophisticated device fingerprinting in place enables businesses to better detect automation that tries to mimic human behavior and obfuscates the characteristics of the device.

Bot Response Strategy: Binary block or accept methods of fraud prevention leave gaps for false positives and negatives. Companies need multiple response options that include challenge and alert strategies in order to weed-out complex attack types.

Machine Learning: Businesses should invest in a sophisticated detection platform that can detect patterns using probabilistic, statistical, and machine learning-based models.

Multi-Layered User Behavior Analysis

As the economic incentive to commit digital fraud increases, so does the sophistication of the methods used to carry it out. This relationship between incentives and attack sophistication has always been present and is one that will likely remain constant forever. While IP intelligence, device intelligence, rate limiting, and statistical learning are all reliable methods to analyze traffic, this will no longer be sufficient in 2022. Businesses will also require user behavioral analysis and behavioral biometrics to strengthen bot and fraud detection signals. Robust user behavior analysis tools can enable them to detect the differences in how a bot interacts with a page versus a human. Businesses will also need deep analysis of a multitude of data points in order to spot sophisticated bot traffic trying to hide as human.

Best Practices for 2022:

Invisible Risk Screening:
Invisible screening makes it possible to deter risky traffic while good users can access their accounts easily and without excessive friction. This multi-layered risk assessments provide the greatest accuracy.

Advanced Behavioral Biometrics:
The events collected from behavioral biometrics can help detect attacks by acting as a supplement of IP or device information, making it easier to detect today's human-like bot attacks.

Drive Up Cost to Evade:
Another benefit of behavioral biometrics is that it takes time, resources, and knowledge of programming – which most attackers don't have — to efficiently spoof behavioral biometric data at scale.

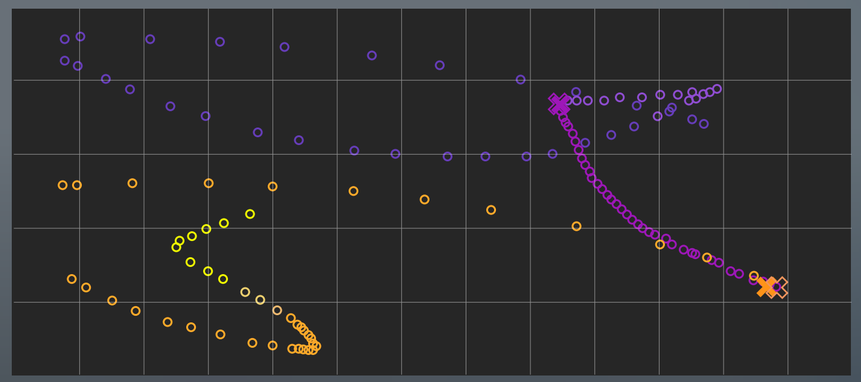
Behavioral Biometrics: Raising the Bar for Attackers

With the prevalence of IP and fingerprint spoofing, behavioral biometrics is a necessary addition to a bot detection strategy in 2022. Analyzing how a user interacts with a device with velocity and accelerometer, data can reveal strong differences between simple automated systems and real human users. Legitimate human behavior is usually complex and chaotic whereas the automated behavior is simple and restricted to what is strictly necessary to complete a task.

The charts below illustrate the stark difference in behavioral patterns when comparing a real human versus a bot. This was taken from an Arkose Labs customer, where we detected malicious bot activity with the help of behavioral biometrics. This complements IP and device assessments, and works across use cases, including account takeover, web scraping and fake account creation.

Differences in Mouse Movements

Real Human



Mouse Motion Click

Bots

Mouse Motion Click

Powerful Challenge-Response Strategy

A challenge-response strategy can be a valuable way to validate suspicious traffic programmatically and alleviate the pain of false positives and reduce false negatives. just like all the attack detection measures you put in place, expect persistent attackers to attempt to circumvent challenges at scale. For example, CAPTCHA-solving services are readily available in the well-connected fraud ecosystem. For increased effectiveness, attackers often will "chain" multiple solver solutions into a single script to perform a variety of functions. With additional time investment, fraudsters can utilize machine vision technology to bypass traditional challenge puzzles using bots. They may also quickly pivot to using fraud farms when their bot attacks meet resistance. Digital businesses need a smarter challenge-response strategy that is custom-built to remain resilient to evolving evasion techniques.

Best Practices for 2022:

Secondary Screening:
To address inconclusive signals, businesses should employ secondary screening that weeds out bad actors, but proves easy for real users to authenticate themselves.

Machine Vision Resilience:
Challenges should be designed against the latest advancements in machine vision technology so they can't be overcome by advanced automated solvers.

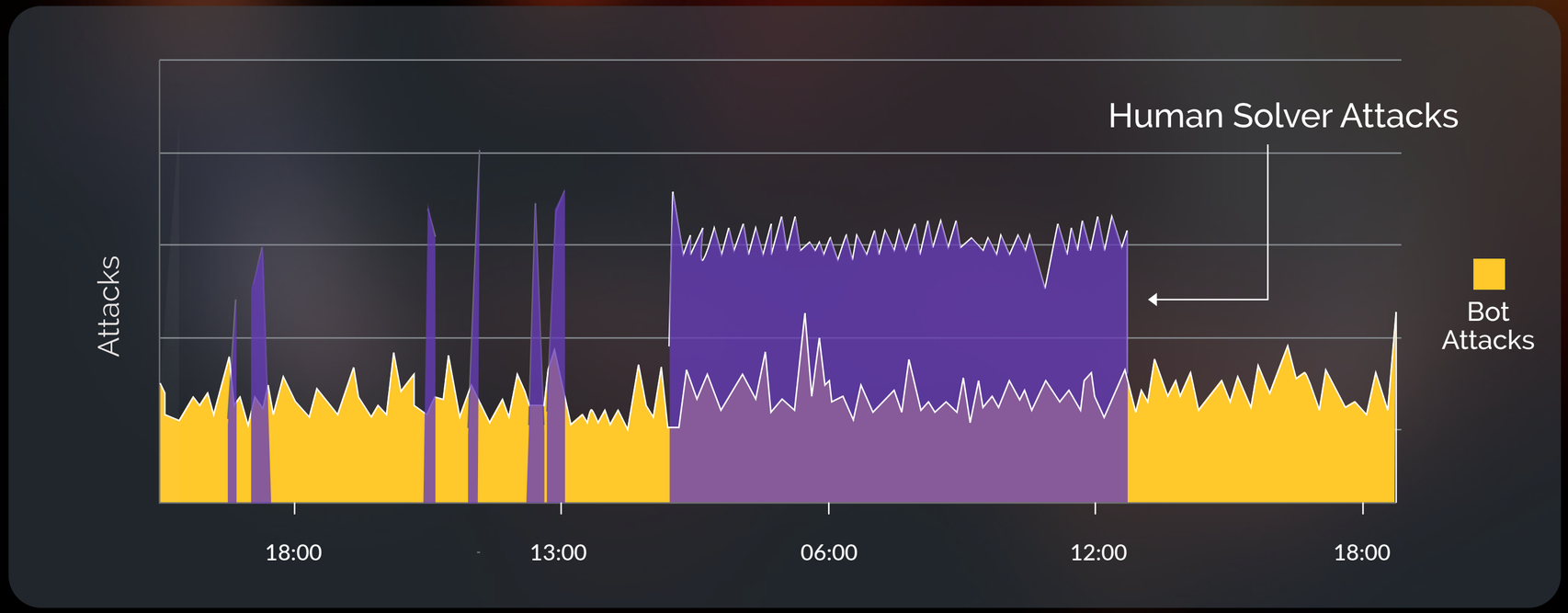
Generated in Real-Time:
Challenges that are generated in real-time and at random to prevent attackers from training bots against certain images or puzzles, making it impossible for attackers to bypass.

Human Fraud Farm Strategy:
Challenge-response strategies should include defenses against both bots and human fraud farms, who are hired to solve advanced anti-automation challenges.

Case Study: Software Provider Thwarts CAPTCHA Solver with Arkose Labs

Arkose Labs helped a major global software firm stop attacks using a CAPTCHA solver service. The client was being targeted with automated attacks actively attempting to solve our image-based challenges. After the automation was stopped by Arkose Labs' custom challenge, the attacker shifted to a "low and slow" attack via a human fraud farm.

Arkose Labs' network of known fraud signals helped to detect this new attack and protect the clients against an attack that they would not have been aware of. This is a common tactic we see as attackers pivot from automated attacks that are stopped by Arkose Labs technology, only to be stymied again by challenges designed to waste human attackers' time until they give up.



Actionable Insights to Work Smarter

Having the right fraud and security technology in place can create great operational efficiencies and allow internal teams to work smarter. Many are overwhelmed with manual efforts to stop attacks, especially at high growth companies that continue to be the target of fraudsters. Talent shortages in the cybersecurity industry and the difficulty all companies face today in attracting and retaining talent are putting more pressure on businesses to scale their efforts and be in a more defensible position against fraud attacks.

To keep with the threat landscape, fraud & security teams need solutions that keep them agile, with actionable insights to respond fast without impacting customers in the process.

Best Practices for 2022:

- **Actionable Insights:**
  With the ability to gain clear visibility into attack patterns, businesses can effectively deploy precious resources where most needed to fight fraud more efficiently.

- **Programmatic Validation:**
  Businesses should have fraud and security solutions in place that do the "heavy lifting" on detection, only leaving the most complex attacks for internal review.

- **Enterprise-wide Collaboration:**
  It's imperative for all organizations to work closely and share information across silos to stop fraud attacks. Infosec, identity and fraud teams should be closely aligned on identifying potential threats and remediating them.

Arkose Labs helped one client decrease support escalations by 84%

Case Study: Arkose Labs Enables Fintech to Stop Attacks and Save Money

Problem: Arkose Labs works with a major fintech client that enables customers to buy and sell stocks, cryptocurrencies, and other financial products. The company was facing digital attacks on a number of different fronts. Attackers were committing ATOs at scale to compromise existing user accounts. This posed a major issue because users were getting locked out of accounts. In the trading world, time is money and having to wait for access to a compromised account to be fixed can be highly frustrating and cost money for users.

Solution: To help stop these attacks, the Arkose Labs detection engine was implemented on the clients web and mobile app flows. It was used to identify and classify bad traffic and pass that information along to the client for remediation. Arkose Labs was also used to ensure that third-party aggregators were complying with the client's policy, and Arkose Labs' tokens were leveraged to track and identify phishing attempts. These tokens were also used to authenticate and protect other API endpoints across the platform. With increased visibility into the attack patterns, the fintech had a leg up on the attackers and and was able to prevent attacks.

Results: Arkose Labs helped the fintech see a 70% reduction in ATO. 6.4 million token replay attacks were identified and stopped during the first week Arkose Labs was live on the platform. By detecting these attacks, Arkose Labs greatly improved the experience for good users while creating significant operational efficiencies, due to far less calls to customer support and less manual effort analyzing potentially suspicious traffic.

Safeguarding the Future of the Digital World

The way we interact with the digital world is evolving. Indeed, as virtual platforms become more prevalent our online identities may become just as important as our “regular” identities. While this holds exciting promise, it also means there are many new digital touchpoints that attackers can target.

That’s why businesses need to plan against not only attacks today – but for the attacks of tomorrow. The intelligent bot revolution will be a game-changer in how businesses need to protect their platforms and users. As fraud and security specialists, we need to be constantly innovating and evolving as a community. We cannot be only reactive and respond to attacks as they happen, but proactively put tools in place to fight them. This means investing in defense-in-depth that cover the full spectrum of attack detection, attack response and advanced analytics, powered by machine learning.

At Arkose Labs, our philosophy is not just to mitigate attacks, but to stop them long-term. We do that by driving up the cost of attacks so much that perpetrators simply give up and move elsewhere. When you provide enough friction to attackers – while ensuring good users pass through easily – you can be assured of having a fraud-free digital platform.

This will be the guiding factor that leads us as we build out more capabilities, and continue to protect businesses and their users across the digital economy - and the emerging metaverse - in the future.

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers the world's first $1 million credential stuffing warranty. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. Headquartered in San Francisco, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, Tokyo, Japan, and London, UK, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast500 ranking.

Offices

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

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

United Kingdom
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Japan
San Jose, Costa Rica
Tokyo

Schedule Demo