Arkose Labs

Ebook

Protecting Media and Streaming Businesses from Fraud and Abuse

Industry Trends and Best Practices

Introduction

Digital media companies have exploded over the last decade, offering services as diverse as news, video streaming, gaming, social media and dating. Online media has been a major disrupter, causing a dramatic shift in the way companies deliver and monetize content and information. The costs required to create and share content are minimal compared to traditional print and broadcasting media. This democratization of content creation means that anyone with access to the internet can participate in politics or conduct business online.

The exponential growth of digital media services has created a highly competitive landscape. Promotional or bonus offers and 'freemium' models are common as media companies battle to attract new customers. These are popular with fraudsters who have been quick to exploit introductory offers, stealing personal data, content behind paywalls, and payment credentials - as well as disseminating spam to billions of potential victims.

20% of all transactions on media platforms are attacks, and in-house fraud teams are struggling to cope with the sheer volume of malicious traffic. This is damaging both business profit and brand reputation, and gives malicious actors the power to influence politics and society for their own ends.

The Media Industry: Key Fraud and Abuse Trends:

It is impossible to talk about 2020 without considering the COVID-19 crisis. The mass lockdowns of entire countries and social distancing measures imposed have forced businesses and consumers alike to move many of their interactions online. Fraudsters have been quick to ramp up operations taking advantage of the explosion in demand for digital entertainment services and social media.

1 in 5
of all media traffic is an attack

60%
of all attacks were on logins

40%
increase in attack volumes in 1H 2020

31%
human-driven attacks

69%
automated attacks

54%
mobile attacks

45%
desktop attacks

Arkose Labs Q3 Fraud and Abuse Report

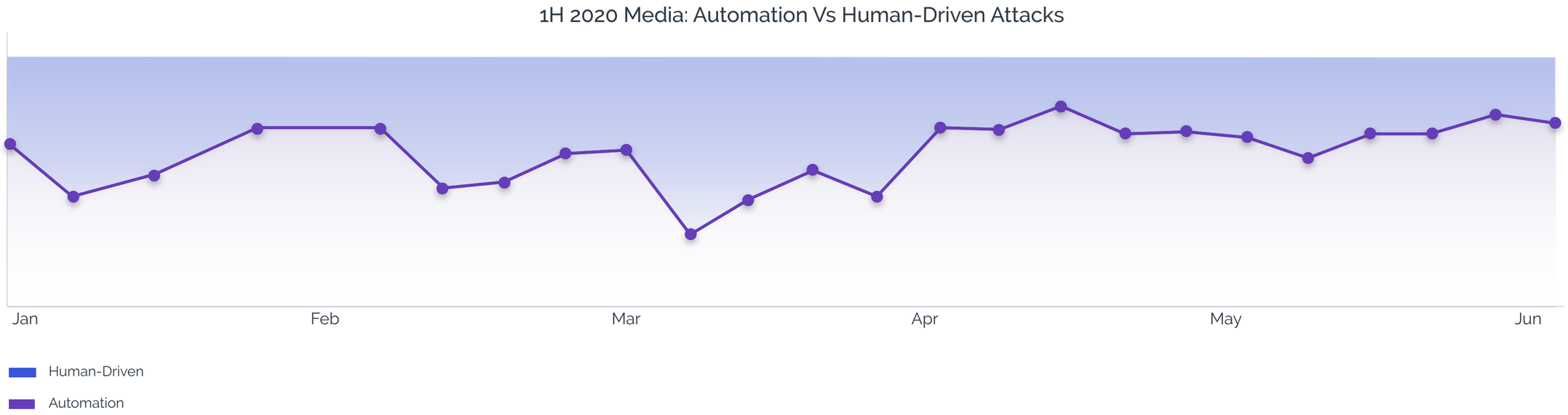
The Evolution of Attack Patterns

Fraudsters are becoming increasingly inventive, experimenting with hybrids of human resources and automated bots in order to maximize profit.

Companies that accept a certain level of fraud as a 'cost of doing business' provide an arena for fraudsters to test and refine their techniques. As fraud prevention strategies have developed, fraudsters have actively tried to reverse engineer these technologies. When they understand what data is used by businesses to differentiate between good and bad traffic, they tailor their attacks accordingly to mask their identity and true intent.

Multi-step attacks are launched using automated tools to lay the foundations, and supported by human labor further downstream. For example on a dating site, large-scale identity credential testing might be used to target the sign-up process, followed by humans based in sweatshops who do more nuanced interaction with genuine customers to launch scams.

These highly sophisticated attacks force fraud prevention teams into a reactive position, as they struggle to keep up with the volume and speed of attacks. It is vital to understand the attack methodology and economic incentives driving fraud to create robust, long-term fraud protection.

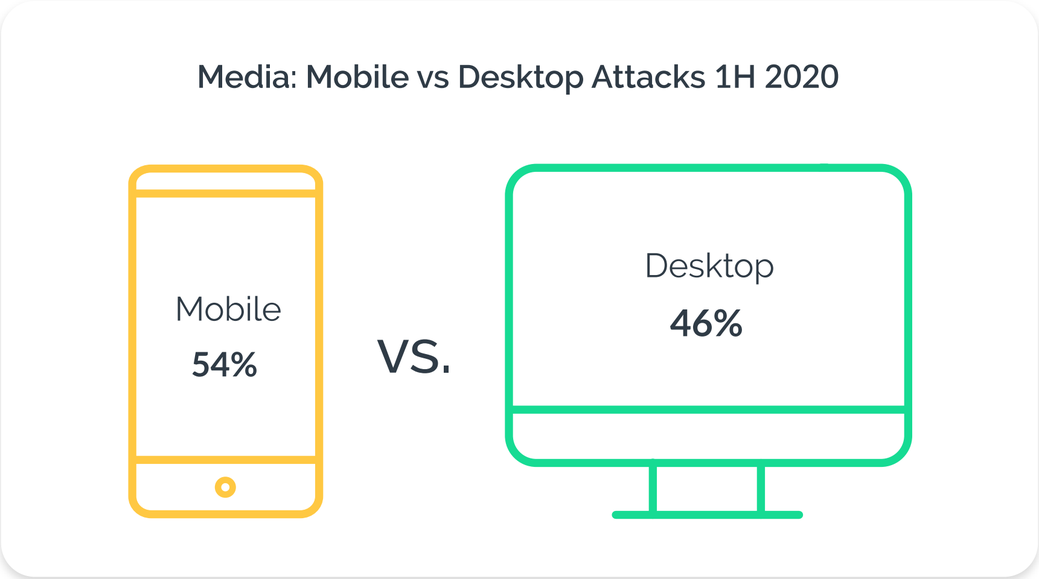


Fraudsters Targeting the Mobile Channel

54% of attacks on media and streaming platforms were from mobile devices in the first half of 2020*. This is compared to an average of just 21% across all industries, making media one of the highest mobile attack rates.

Social media in particular sees a high volume of mobile traffic: the platforms have a young clientele who expect easy access to platforms via apps. These apps tend to be user-friendly and friction-light as creators compete for business. Fraudsters are all too aware of this, and are focusing attacks on mobile channels.

Sweatshop workers are major players here, operating multiple mobile devices simultaneously to launch large-scale attacks on media companies. Human fraudsters are particularly useful in bypassing anti-fraud measures designed to root out bots, and effectively mimic genuine customer behavior. Fraud prevention strategies need to work seamlessly across channels and be designed to prevent human, automated and hybrid attacks.

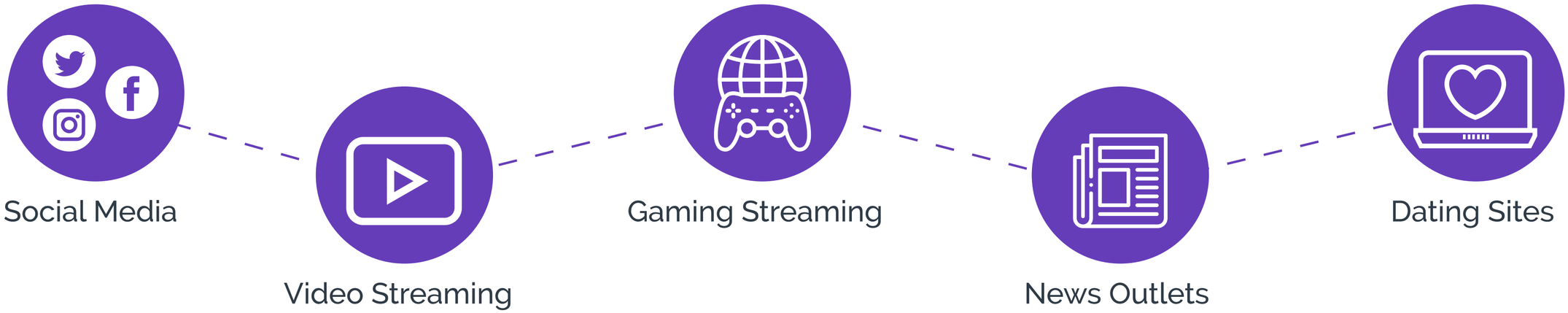


Digital Identity in a Post-Truth Era

In a post-COVID world, even the most tech-resistant have moved online. Consumer data is the most prized commodity for fraudsters and it has never been easier to access.

In the evolution of digital media, identity data is key in accurately differentiating between trusted or fraudulent traffic. Fraudsters recognize this, and have adapted their attack models using widely available identity toolkits to impersonate trusted users and disguise malicious intent.

Data breaches are now so common that consumers have become desensitized to the risk, often using simple passwords across multiple platforms. Victims of fraud do not realize they have been targeted until a bill arrives for something they haven't bought or they experience trouble with their credit rating.



The Many Faces of Media Fraud and Abuse

Account Takeover

Fraudsters takeover legitimate accounts and use them for cyber crimes including spam, money laundering, account draining, and credit applications. 20% of login attempts on the Arkose Labs' network were ATO attacks at the start of 2020.

False Information

This is the deliberate spread of hoaxes or disinformation, and has massively increased with the growth of social media platforms. The intent is usually to discredit people or agencies, or to gain financially or politically.

Fake Reviews

Fraudsters generate thousands of fake reviews to influence purchases and receive financial kickbacks. Authentic reviews are outnumbered, creating a false perception of the business landscape. 86% of customers read reviews before making a purchase.

New Account Origination

Stolen or fake identities are used to create new accounts en-masse. Fraudsters then abuse bonus offers and free account trials, as well as selling them on for further crime including spam and credit abuse.

Ad Fraud

Fraudsters target the billions spent each year on digital marketing strategies. This ranges from click farms exploiting pay-per-click campaigns to fake 'influencers' with a large 'bot' following who are paid large sums for ads.

Election Tampering

International election interference is increasingly problematic with troll farms creating thousands of fake social media profiles supporting political parties and disseminating false information and fabricated articles. This perpetuates political echo chambers and threatens democracy.

Account Takeover - A Gold Mine of Valuable Data

Account takeover is a lucrative form of fraud with a long shelf-life: just one compromised account can lead to a wide range of related attacks. As with most fraud, the financial incentives are key, with fraudsters using accounts to siphon funds, redeem reward points and access saved passwords and payment details. Breached accounts will often be sold on to multiple users creating a pyramid scheme of account takeover.

To maximize financial gain, attacks are complex and targeted, using a combination of automation, human labor and location spoofing tools to mask identity and intent. Attackers often play the long game, with many accounts remaining dormant for months after they have been breached. This makes it very difficult to detect the source of the breach and stop further fraud downstream.

Media and streaming accounts are increasingly attractive to fraudsters as they diversify their products. They have always offered a wealth of personal information as well as the opportunity to push products and political agendas. However many social networking platforms now have marketplaces and are introducing P2P payment services which massively increases the potential for profit from account takeover and the associated crimes.

Fraud prevention teams are often left trying to manually identify and shut down these attacks, which is labor intensive and costly. Businesses need automated solutions that spot this fraud early on in the life cycle and prevent large-scale attacks.

Media Platforms in the 21st Century: Adapt to Survive

As huge numbers of new competitors join the market, digital media services are seeking new and innovative ways to engage with users. As a result, media platforms are diversifying to offer multiple service from gaming to music streaming. These live streaming services are rapidly growing in popularity, making them increasingly attractive to cybercriminals.

Case Study: Caffeine.Tv

Caffeine is a social broadcasting platform streaming live videos in the entertainment, gaming and esports sectors. It attracts a tech-savvy clientele who expect a sleek interface, design and seamless user experience.

The Problem:

Caffeine.tv had been working with a legacy spam and abuse solution on account registration, which was easily bypassed by bots. Bogus accounts were used to interfere with live streaming videos and disseminate spam disrupting user experience.

The Solution:

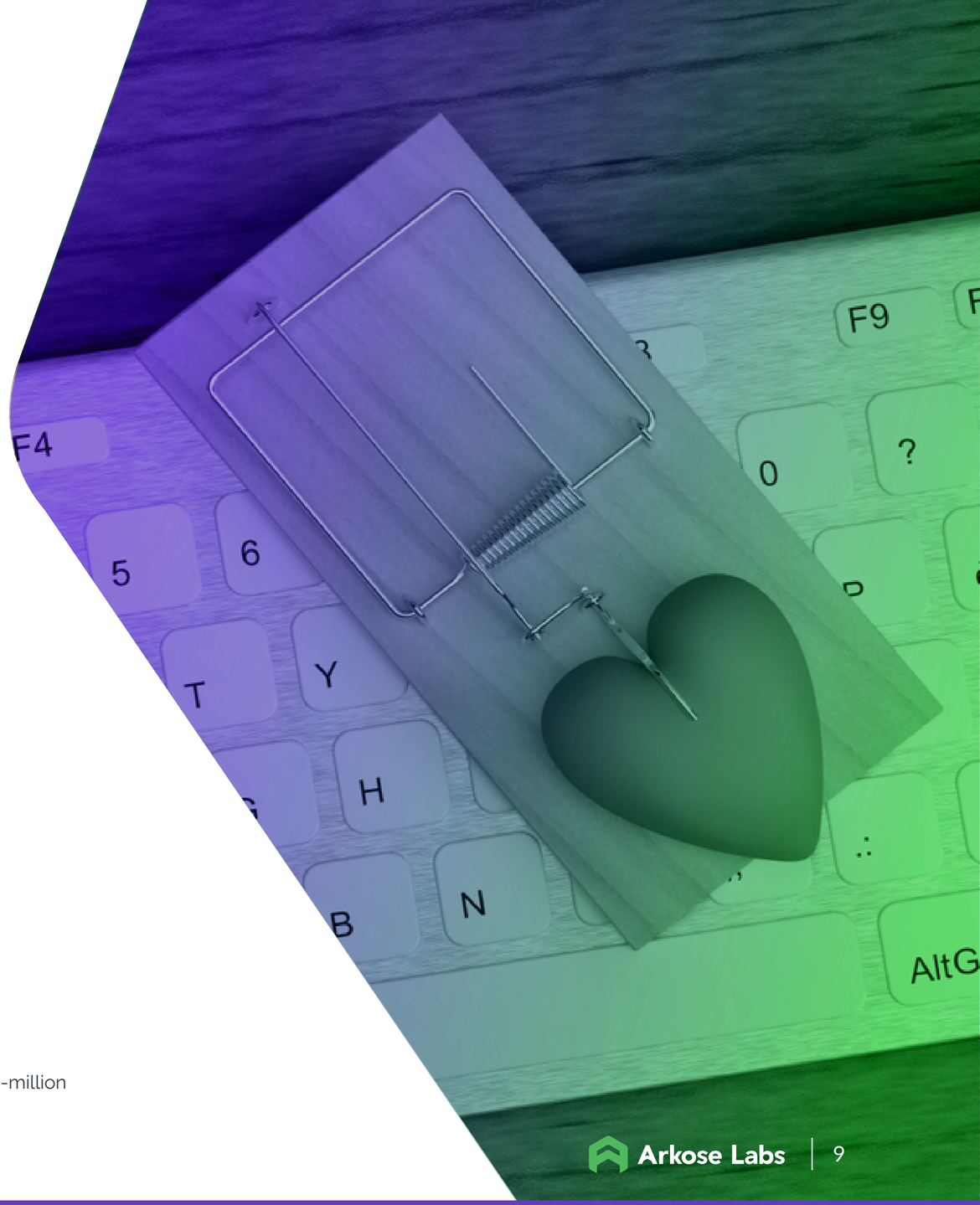
Arkose Labs analyzed factors including device ID, IP address and location, looking for anomalies that indicated bot activity. Suspicious traffic was directed to tailored challenges designed to weed out bots and determine intent. Attacks were eliminated restoring user experience and business reputation.

Spotlight On Online Dating

Dating fraud has one of the highest attack rates across social media platforms. A recent report from Arkose Labs found that 2 in 5 of all logins were fraudulent and a separate government report found that in the US, customers lost more than $201 million to romance scams in 2019*.

Around 50% of these attacks are human-driven; the high potential ROI justifies the inflated cost of human labor. Scammers create impressive profiles posing as professionals e.g. 'doctor' or 'soldier' and build relationships with genuine users over time. Once trust is established, they ask their 'dates' for money for everything from medical expenses to gambling debts. They tend to request reload cards or gift cards which allow them to remain anonymous, are impossible to reverse and provide instant access to funds.

Automated attacks on dating platforms focus on scraping content and identity details, stealing information and disseminating spam and malicious content. It's clear that dating companies need an innovative fraud prevention solution that stops both human-driven and automated fraud.



https://www.ftc.gov/news-events/press-releases/2020/02/new-ftc-data-show-consumers-reported-losing-more-200-million

Case Study: Romance Scams

The Problem:
A popular global dating platform was experiencing high levels of human-driven attacks where bad actors created fake accounts and scammed genuine users. They spammed real users with malicious links, requests for money and phishing scams. Legitimate customers faced significant disruption and were increasingly
dissatisfied with the service.

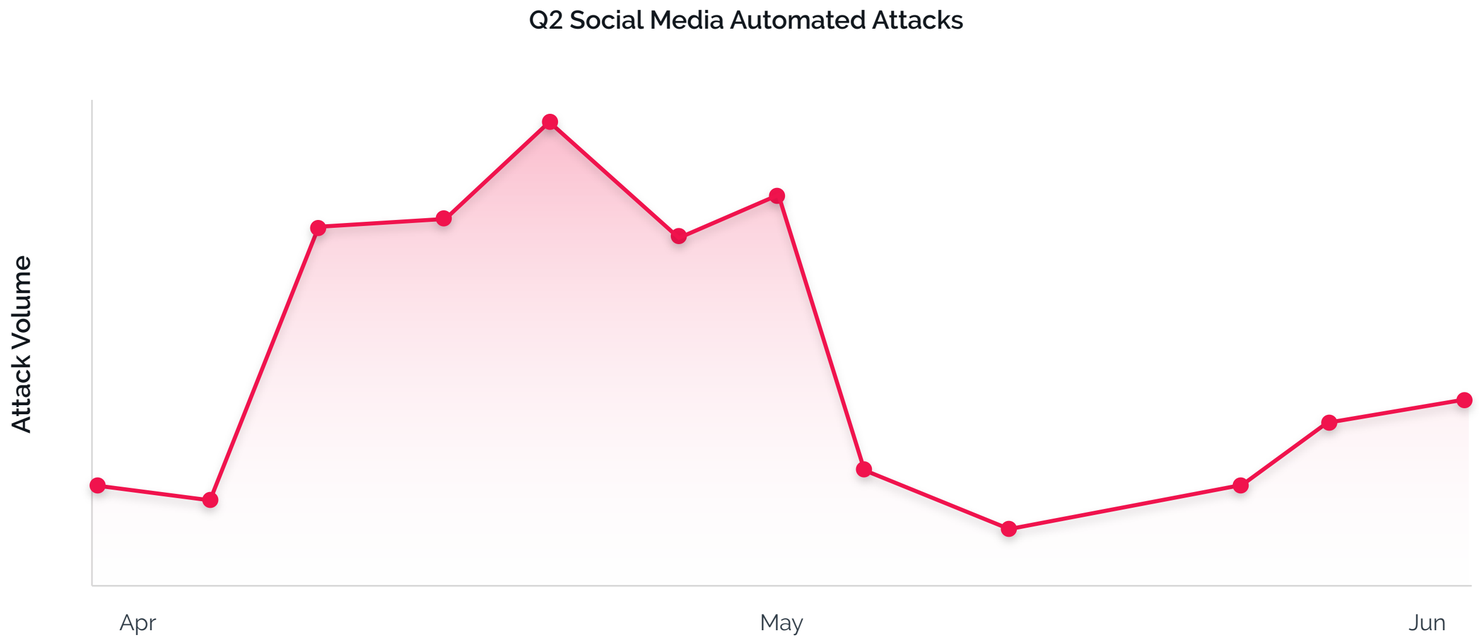
The Solution:
Arkose Labs used advanced behavioral analytics to identify suspicious activity at the account creation stage. Risky traffic was presented with targeted friction that removed the profit potential and deterred fraudsters from creating the accounts.

The Results:
The platform saw an 80% reduction in fake account registrations, preventing downstream spam and abuse. Customer satisfaction was high and company reputation saved.

Social Media: A Battleground for Bots

There was a spike in bot-driven activity across social media platforms in April and May 2020. Bots are used in attacks to scrape content, launch scams or disseminate false information. Social media sites can be used to spread propaganda and use hashtag hijacking and trend-jacking to influence political and social discourse. They are used by a wide range of actors with very different goals. For example ISIS have used similar tactics to recruit major music stars. Building both good and bad bots is increasingly easy, with individuals with very different motivations, connected to politicians, businesses and nation states, suspected of leveraging these tactics.

This is becoming a battlefield, with people watching from all sides to capitalize on the latest bot technology. This issue will be under increasing scrutiny as the COVID-19 lockdowns and the US presidential election continue to dominate public debate.



The Weaponization Of Social Media

Social media platforms have far outgrown their origins as places to connect. They are global businesses facilitating news, entertainment, peer reviews, and financial transactions. The way people interact with the digital economy has shifted dramatically, as they rely increasingly on their peers for information on everything from politics to purchases. Fraudsters, legitimate businesses and governments are all leveraging this to their advantage, capitalizing on a trusting digital audience, and social media platforms who are not bound by the regulations of traditional media organizations.

The Rise of Computational Coercion and Propaganda

Computational coercion is a form of cyberattack that manipulates user data to control how information is ranked, filtered and distributed in the digital economy. This undermines the integrity of customer interactions, subverting algorithms to influence consumers' political and social beliefs and purchase choices. The primary motive is profit, with fraudsters weaponizing user data to take advantage of a range of incentives including cash-based commissions, reward points and discounts.

The revenue made through social media platforms has shot up over the last decade and as they increase their scale and reach, will continue to grow. It is crucial that platforms act to protect the integrity of their content and users against fraudsters.

Content Scraping: Targeting the Crown Jewels

We are living in an era where media companies base their entire business models on the commodification of data and content. Fraudsters target media platforms with malicious scraping attacks where bots steal user data and content. This poses a serious threat to profit. Companies need a robust fraud prevention strategy and a zero-tolerance approach to prevent scraping attacks.

The Problem:

A major social media platform used primarily for networking, sharing content and job postings was facing large-scale attacks from fraudsters looking to scrape information from the public profiles of real users to create synthetic identities or launch targeted phishing scams. The platform's main revenue stream comes from offering products to third parties based on user information so these scams were draining millions in potential revenue.

The Solution:

Arkose Labs was deployed on the website to detect automated bots carrying out scraping attacks and prevent malicious activity. When behavior was flagged as potentially suspicious, it were presented with enforcement challenges that increased in complexity in order to sap the time and resources of potential fraudsters slashing the ROI of the attacks.

The Results:

Automated attacks were completely eliminated and there was a 22% reduction in scraping. Good customer throughput increased by 19% and the overall customer experience was improved and safeguarded.

Step 1 Analyze Real-Time Signals

Media and streaming companies need multi-layered protections in place to protect against the various forms of abuse they are targeted with. Risk-based authentication should analyze behavior patterns and flag suspicious activity for secondary screening. However in the post-breach era where identities have been corrupted en-masse, it is vital that fraud prevention systems do not take data purely at face value.

Deep Device Analytics

Use detailed device fingerprinting and validation to gain an in-depth profile of user characteristics and assess the validity of the device

Abnormality Detection

Monitor networks for anomalous events or trends, and analyze network traffic patterns in real-time to identify suspicious behavior patterns across multiple platforms.

Network Intelligence

Compare data in real-time across networks to identify known bot and sweatshop activity.

Machine Learning

Detect malicious activity displaying similar characteristics across different use cases and times using machine learning.

Location Assessment

Authentically identify location spoofing, and analyse whether activity is proportionate to authentic traffic associated with location.

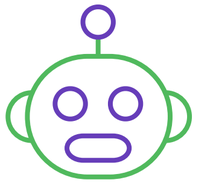
Step 2 Interactive Challenges

Friction has traditionally been seen as the enemy of customer engagement, and businesses have focused on offering a seamless user experience. The lack of friction has enabled fraud to flourish as fraudsters evolve their tactics with every attempted attack. This damages company profit and user experience. User-friendly friction can be an ally in both the fight against fraud, and customer relationships. Friction should be graded according to risk:

All challenges should be designed to be easily completed by genuine users to preserve good throughput rates. Targeted challenges waste the time and resources of fraudsters and dramatically slash the potential ROI forcing them to abandon attacks and go elsewhere.

Light Touch

Use interactive technology to test computer responses and ask users to complete very simple challenges.



Bot Challenges

Deploy user challenges that cannot be solved by bots or machine vision software

Sweatshop Challenges

Incrementally complex challenges targeted according to user profile. Use timed mode and multiple challenges to flag and frustrate sweatshops.

Step 3 Monitor Behavioral Patterns

The signs of fraud can be subtle, but sweatshops and bots show very different behavioral patterns to legitimate customers. Real-time device data is a powerful indicator of user intent, but is only one part of the story.

Real-Time Data

Monitor behavioral patterns including pressure, keystroke, motion, swipe patterns and navigation to create digital 'telltales' that provide detailed clusters of information for each user session.

User Action

Analyzing user behavior patterns is an important signal of potential malicious activity. Bad actors are motivated by profit incentives and typically fill out forms quicker, copy and paste data and move more quickly than genuine customers to complete tasks at scale.

Challenge Interaction

Using interactive enforcement challenges provides further valuable insight into user behavior. Time to solve challenges, how an image is rotated, and the mouse-cursor trail can all be telltale clues of true user intent.

Shared Network Information

Fraud prevention systems will benefit from evaluating fraud data across a network of websites and apps, allowing them to flag suspicious users in real time.

The Arkose Advantage

The Arkose Labs Fraud and Abuse Defense Platform offers complete protection against both human-driven and automated fraud. It is designed to balance optimal user experience with robust security.

This two-step platform combines Arkose Detect, a dynamic risk engine that analyses traffic for signs of fraud in real time with Arkose Enforce, which provides a wide range of step-up challenges tailored to the user's risk profile.

When the platform detects suspicious behavior, the user is presented with a series of increasingly difficult challenges that waste time and resources rendering the attack expensive and unsustainable. Depending on the behavior patterns and data profile, challenges can be either time limited to eliminate queued pipelines or extended over a long period of time, draining user efficiency.

Arkose Enforce uses 3D visual puzzles which are not solvable by bots; Arkose Labs is the only fraud prevention platform to offer a 100% SLA guarantee against automated fraud.

Arkose Labs: A Competitive Edge

Step-Up Challenges Thwart Attacks.
Fraudsters must waste increasing time and resources completing challenges, dramatically slashing the ROI and forcing attackers to abandon the assault.

Customer Relationships Are Safeguarded.
If a genuine user has been categorized as risky, they can confirm their identity by demonstrating normal behavioral biometrics and completing challenges.

Bot Beating Approach.
Unique, evolving challenges weed out bots early in the process. 3D puzzles are not solvable by computer software and machine learning techniques.

Good Throughput For True Customers.
All users are offered the chance to prove their legitimacy so no good actors are blocked.

Easily Integrated, Cost Effective Solution.
The authentication process is incorporated into the platform and not reliant on SMS or other out of band processes.

Unified Risk Decisioning And Step-Up
End to end platform which combines risk assessments and secondary screening, with a continuous feedback loop to refine and improve results.

Conclusion

Media and streaming services provide a treasure trove of data and content, and dynamic communication platforms for malicious actors to abuse. The expectation that fraud is 'a cost of doing business' has left fraud prevention teams in an endless game of 'cat and mouse' with fraudsters and is costing businesses trillions worldwide every year.

Media and streaming services are expanding in multiple directions in the bid to attract and retain a loyal customer base. The diversification of products on offer has opened up many new potential profit streams for fraudsters. Fraudsters have benefitted from years of 'training' through previous attacks and data breaches, and the sheer volume of attacks is putting huge pressure on in-house fraud teams.

The effects of fraud are far-reaching and have great potential to cause social, political and economic damage across the globe.

Ultimately fraud must be seen as a business: fraudsters' primary goal is always to make the highest profits in the shortest period of time. Fraud prevention strategies should focus on eliminating the ROI of attacks. Detailed risk profiling combined with targeted authentication challenges ensures that the right level of friction is directed to each user. Good customers easily clear challenges while fraudsters waste time and resources making attacks unprofitable. This renders the attack economically non-viable and forces fraudsters to go elsewhere.

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 Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo