Arkose Labs

Ebook

Hitting the Fraudsters Where it Hurts: Their Wallets

Financial Motivation Fuels All Fraud

Financial Motivation Fuels All Fraud

Fraud is more profitable than ever before. Attackers continue to get more cunning, and increase their understanding of the procedures and defenses that businesses have implemented to stop them.

The amount of effort and resources a fraudster expends on an attack is ultimately driven by the monetization potential. Once fraudsters hit a certain level of resistance, this begins to erode their ability to carry out the attack while still preserving ROI. This is the point where most attacks drop off.

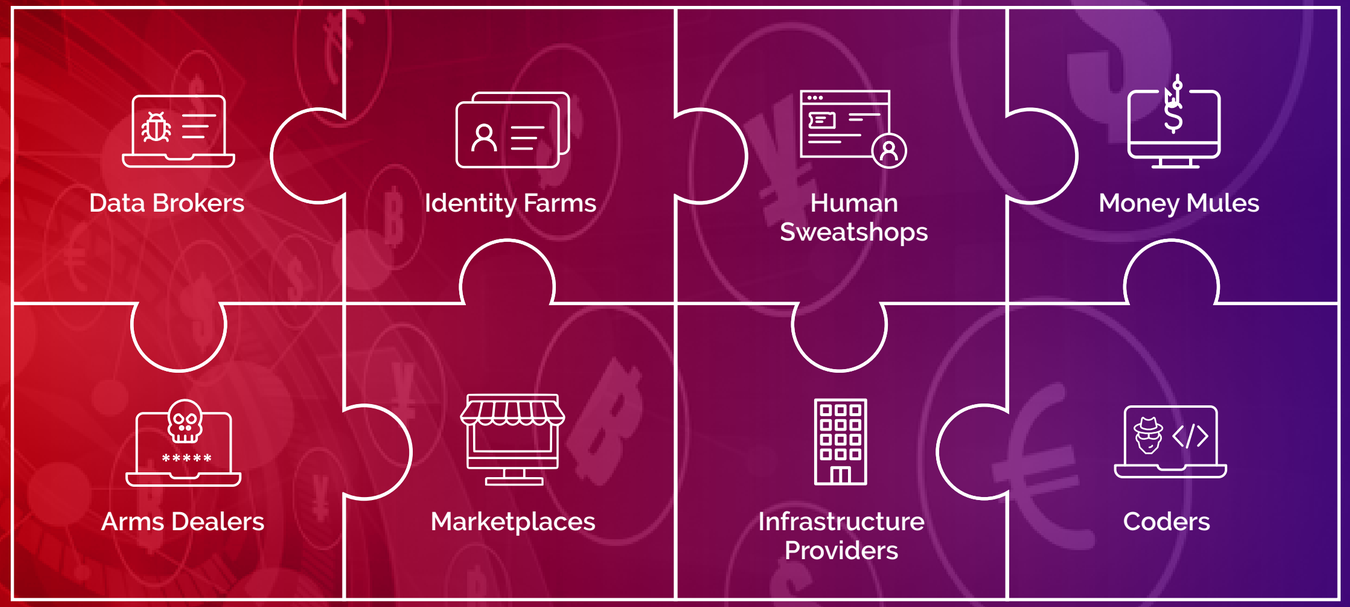
In order for businesses to create effective fraud defense strategies, they need to better understand the economic incentives behind fraudsters' activity. Long term fraud prevention lies in derailing those economic drivers and make it too costly to attack. Fraud prevention has honed in on assessing users by their digital identity, based on the devices they use, the locations they transact from and their associated identity credentials. However, in a world where data breaches are commonplace and digital identities have been corrupted at scale, a new approach to combat fraud is needed.

The Fraud Ecosystem

Fraudsters have a wide set of services and solutions available to them, which enables them to tap into low-cost resources and toolkits from across the globe. This is how they carry out attacks at scale, far beyond the capacity of a single human working alone.

For example, data brokers and identity farms work together to create very comprehensive identity profiles, or synthesized identities that use fragments of legitimate credentials that can be effective in attacks.

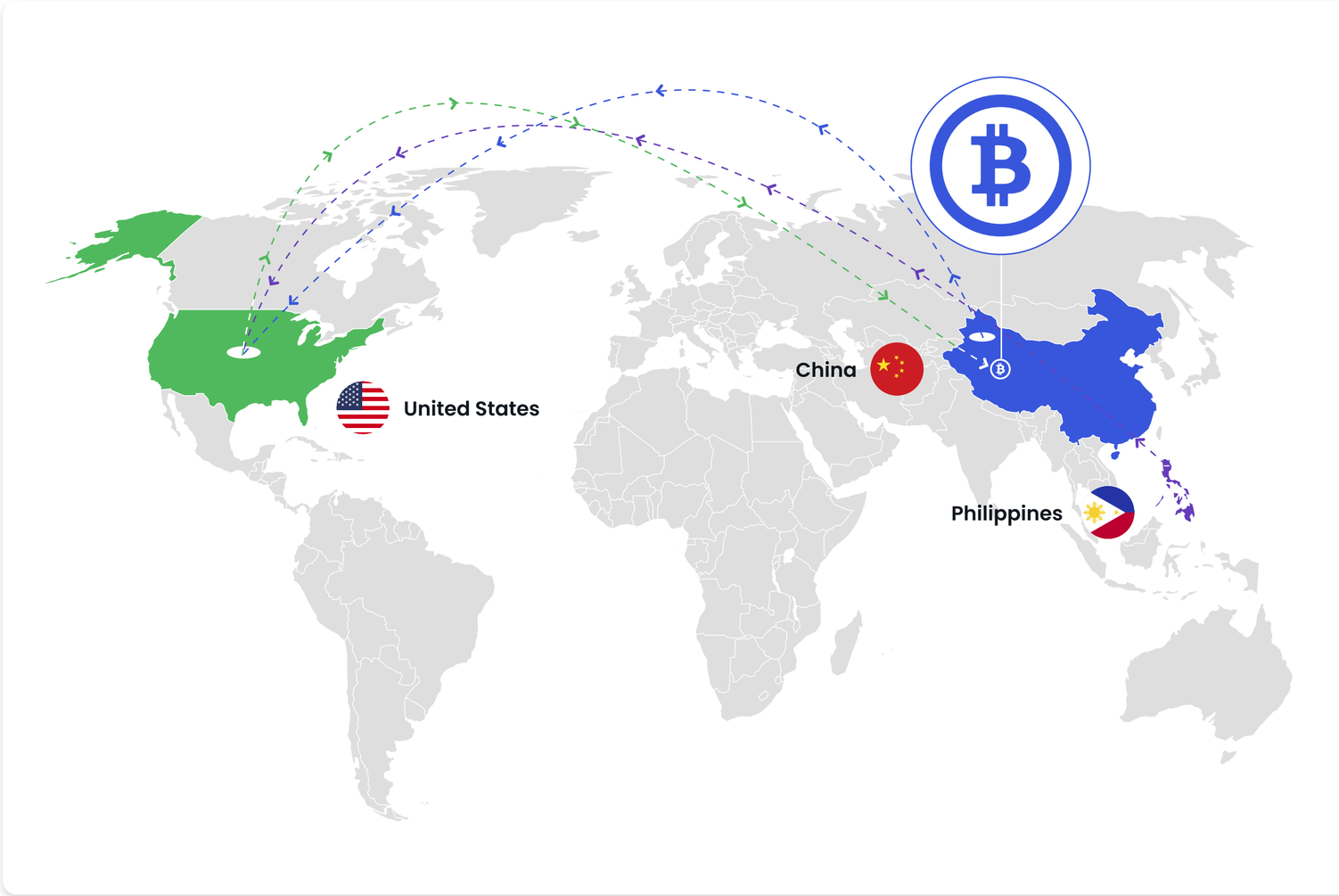
This fraud ecosystem also includes “click farms” or human sweatshops around the globe. These are teams physically working together, or through distributed networks which are connected through apps or marketplaces to carry out attacks at scale. With a fraudsters’ specific goal being to evade authentication steps and challenges, this ecosystem works in their favor.



Case Study : Promo Abuse on a Global Tech Platform

An example of the wider fraud ecosystem at work is the malicious activity that was detected on one of the tech companies Arkose Labs works with. In this case, the customer saw attackers using scripts and humans using identity farms to create fake accounts that were used to mine Bitcoin. Attackers deployed bots to open new accounts at scale and accrue all the free credits and server time that was offered in new account promotions. Specifically, many fraudsters used this free server time for bitcoin mining, which can be a highly profitable but energy-intensive effort.

Arkose Labs identified and stopped the creation of malicious new accounts, using a mix of real-time risk assessments and interactive enforcement challenges.



Results

- 90%+ reduction in promotional credits abuse
- Stamped out bot-driven attacks
- Better overall experience for good users

Global Socio-Economic Factors Driving Fraud

The foundation of the cybercrime ecosystem is based on several global socio-economic factors. These factors create incentives for committing fraud in certain parts of the world. In regions with low costs of living and weak currencies, individuals stand to gain a great deal by attacking US businesses and will be willing to expend more effort on attacks, while still preserving ROI.

On top of the economic drivers, different regions across the globe have different access to the technology that is needed to support sustainable cybercrimes and launch large-scale fraud attacks. Countries with very low internet penetration rates are unlikely to become major fraud hubs.

Wages & cost of labor

Employment rates

Cost of living

Currency disparity

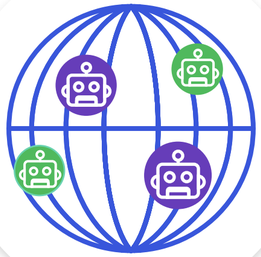
Access to technology

The Human-Driven Fraud Continuum

Companies are increasingly facing complex, hybrid fraud attacks that are launched by fraudsters who combine intelligent, automated bots with a network of human sweatshop resources. The bots are designed to recognize challenges that require human interaction. Where there is high-profit potential, bots redirect these challenges via applications to sweatshop networks, where workers complete the authentication process.

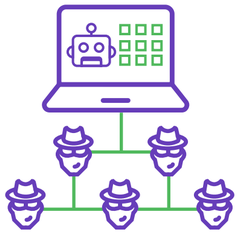
Lone fraudster plans attack and coordinates the required resources.

Lone fraudster deploys large-scale attacks using bots.



When automated attacks meet resistance, bot is coded to escalate to a human.

Bot connects to applications which connect fraudsters to distributed sweatshop resources.



Sweatshop workers complete authentication challenges.

Case Study: Gift Card Fraud

One of the premier distributors of prepaid card and gift card programs was targeted by a major sweatshop operation. The customer was being attacked by a combination of humans and automated bots that was amounting to tens of thousands of assaults daily.

Fraudsters can easily profit from prepaid cards, gift cards and cash because they are not easily traced. They are drawn by the fast reward system which is why there was an increase in attacks.

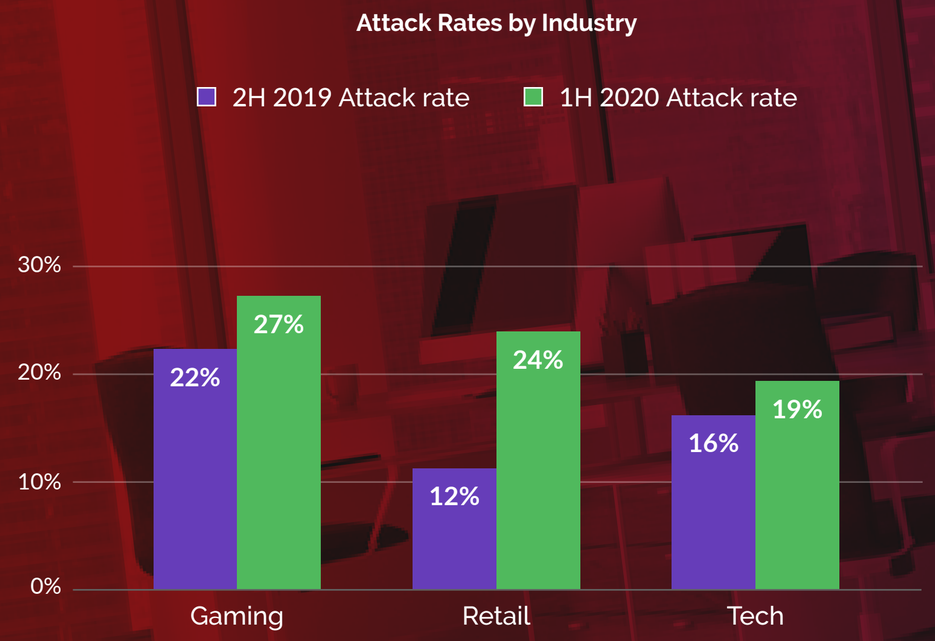
98% reduction in bot attacks

98% reduction in human-driven fraud

Solution

- Arkose Labs platform distinguished good from bad users with no impact to good customer throughput
- Enforcement challenges stopped bots entirely and removed the efficiency of human click farms
- The company continued to work with the Arkose Labs team to find improvements from the data collected

The Most Highly Targeted Industries



E-Commerce

The eCommerce industry is seeing the biggest jump in attack rates, which is due to both the increased online activity and increased profitability of inventory hoarding and scraping

Gaming

The typical spikes that used to only happen on weekends and evenings are occurring everyday, which has also lead to a concurrent rise in attack rates.

Tech

Personal and professional communications and collaboration has moved online. This has increased traffic of new and returning users and the emergence of new sub-sectors like EdTech.

Comparing the Balance Sheets

In the face of this global cybercrime network, businesses have deployed a range of solutions to protect against attacks. The cost of these tools, however, can outweigh any benefit they provide in slowing down fraud.

Fraudsters have economics on their side and are able to tap into different tools while keeping costs low within regions with very low overhead. Cybercriminals are consistently driving profits through their fraud ecosystem. At the same time, businesses have increasing demands on their fraud budgets and personnel.

The Cybercrime Cycle of Success

The more successful attacks that take place, the better the fraud community's ability to launch future attacks. As a result, fraud attack rates are steadily rising –despite the numerous anti-fraud measures deployed in many digital businesses.

Fraud levels will continue to rise indefinitely unless companies stop tolerating fraud as a 'cost of doing business'. Allowing for a certain level of fraud within your online operations actively feeds future attacks, by allowing fraudsters to continually improve their ability to launch and expand successful attacks.

Preliminary attacks

Test stolen data & newly purchased toolkits

Larger-scale attacks

Target more business with verified data and toolkits

New data & more sophisticated toolkits

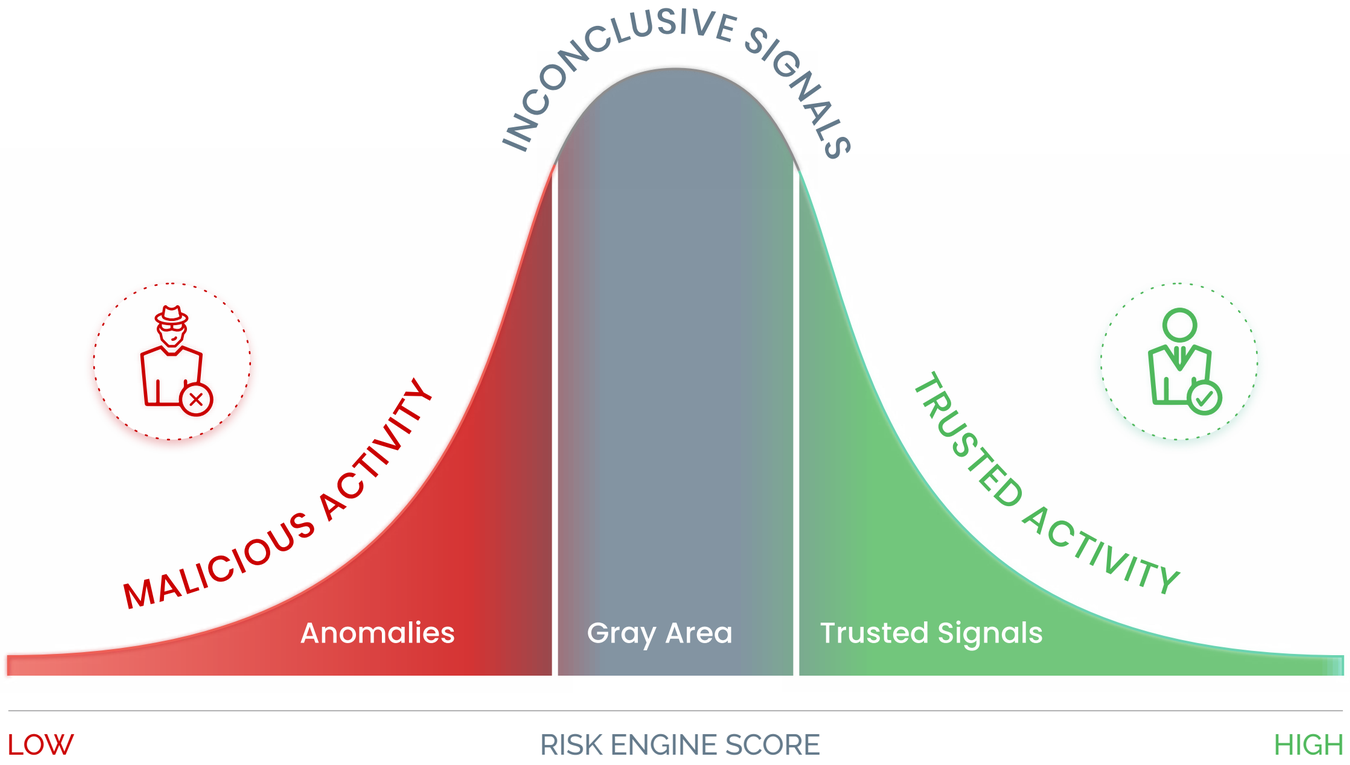
Proceeds used to buy fresh credentials and new toolkits to evade anti-fraud measures

Increased attacks from multiple perpetrators

Knowledge-sharing among fraudsters on tools & techniques which are effective spurs on increased attacks

The Growing Gray Area

Since the beginning of the COVID-19 crisis, businesses have genuine customers that are acting erratically and online consumer behavior has been in flux like never before. This means it has been increasingly harder to baseline what trusted user transaction patterns look like. Attackers are using more sophisticated tools and bots which more accurately mimic human behavior with increasing sophistication. Relying purely on data—driven systems leads to a growing gray area, of traffic falling between "good" and "bad". Without secondary screening of this suspicious traffic, organizations struggle to action the insights from data-driven fraud detection systems.

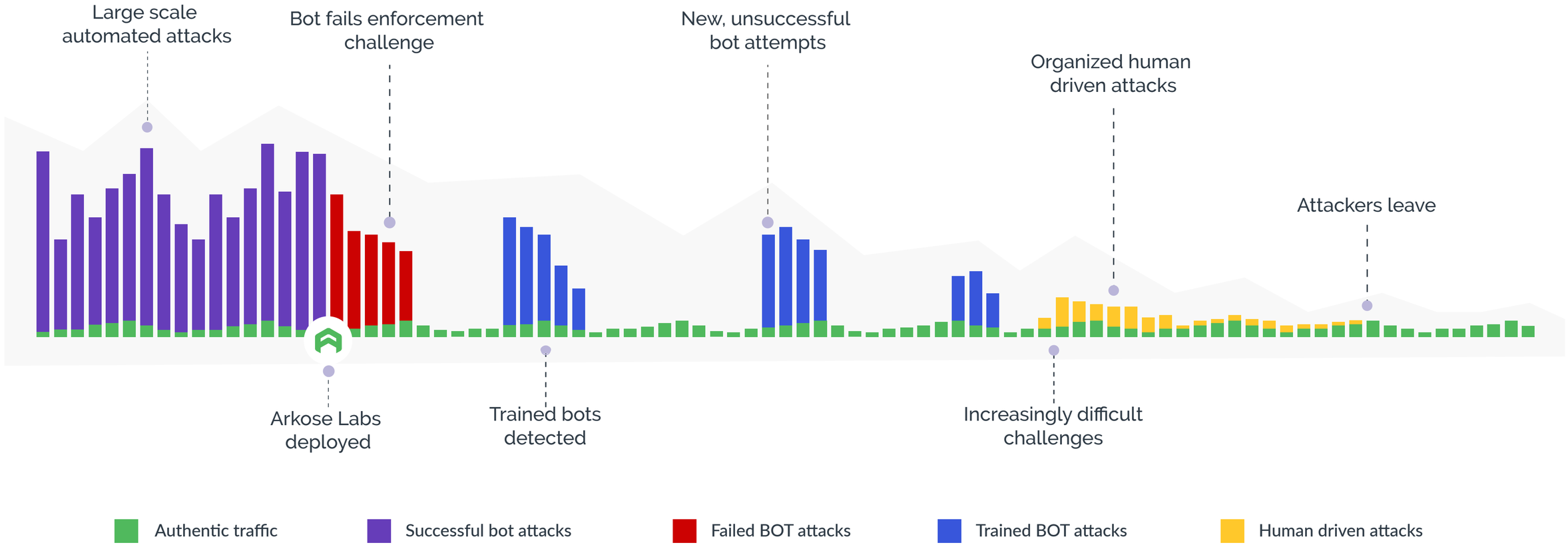


Spotlight on Gaming

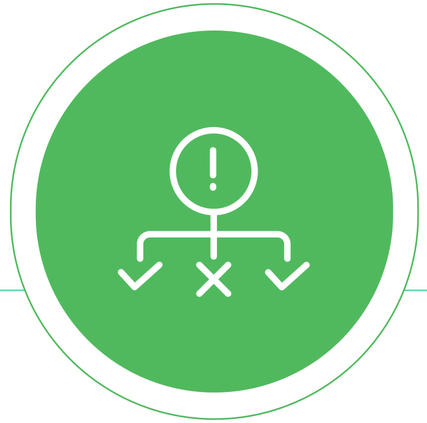
Take online gaming as an example: The amount of fraud committed during the COVID-19 crisis in the gaming industry is seeing a drastic rise, as more users flocked to gaming platforms during quarantine. The types of attacks and routes to monetization are increasingly far reaching, and inventive. For example, Arkose Labs saw a 60% increase in in-game abuse in the first half of 2020, with bots and sweatshops carrying out malicious activity at scale, such as real money trading.

Breaking The Fraudsters' Economics

Arkose Labs has developed a system that effectively undermines the ROI behind attacks. When bot activity is detected by the risk engine, 3D interactive challenges are presented. These are not solvable by machine vision technology, and cause automated scripts to automatically fail. Trained bots are thwarted by swapping out the challenge. When sweatshop activity is detected, the complexity of a challenge is increased which slows attacks down, until the ROI is undermined and they abandon attacks.



Key Advice For Hitting The Fraudsters In Their Wallets



Determine Intent and Behavior

- Real time risk assessment
- Behavioral biometrics
- Triage traffic based on intent

Challenge and Interact

- Interactive challenges eliminate bots
- Sap fraudsters' time and resources
- Behavior and time to solve

Analyze and Learn

- Continuous feedback loop
- Embedded machine learning
- Challenge fewer good users

Conclusion

As we have seen, it isn't very difficult to launch fraud attacks at scale for a minimal investment of money. As long as the rate of return works in their favor, fraudsters will continue their lucrative game. They only need a small percentage of their attacks to be successful in order to be profitable.

That's why traditional methods of fraud mitigation are no longer sufficient. They are plugging holes in a leaking dam. Instead, to truly stop these attacks, businesses need to bankrupt the business model of fraud. By rendering fraud attacks unprofitable, fraudsters will look elsewhere.

While many businesses have come to accept fraud as an operational cost of doing business in the digital age, Arkose Labs believes that the only long-term way to stop cybercrime is to adopt a zero-tolerance approach which focuses on disrupting the economic drivers of fraud. With no economic incentive to attack, fraudsters will eventually abandon their plans.

In a world that's more digital than ever before, it is critical that businesses root out the drivers of fraud, rather than simply trying to mitigate it. That will ultimately lead to a safer and more secure 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 © 2020. All Rights Reserved

Offices

San Francisco
250 Montgomery St 10th Floor, San

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo