Arkose Labs

Financial Trading Platform Protects Accounts From Phishing Attacks with Arkose Labs

CASE STUDY

Customer:

Rapid-Growth Fintech Platform

⚠ Business Problem

- Phishing and vishing attacks targeting users
- Company had difficulty identifying compromised accounts
- Internal teams overwhelmed dealing with attacks

Solution

- Arkose Labs deployed on web and app flows
- Accurately differentiated attacks from good users
- Worked with client to tune defenses as necessary

Results

- Successful phishing attacks reduced by more than 99%
- 6.4 million token replay attacks stopped
- No impact to good user throughput

Overview

The client is a major fintech company that enables customers to buy and sell stocks, cryptocurrencies, and other financial products. It has millions of customers around the world and is known for its intuitive interface and robust digital app. With a rapidly increasing customer base, the firm needed a fraud prevention and security solution that would keep its platform safe and not slow down their users from real-time trading.

The Business Problem

In 2020 retail trading reached new highs of popularity. During this time, the company's growth far outpaced its security capabilities. In fact, traffic levels had increased by 20 times what the company was used to dealing with. This influx of new users created a prime target for attackers, who flocked to the site to target real users with phishing attacks.

Users were targeted in a number of different ways. One common phishing tactic was fraudsters sending a fake text message or email to real users, purporting to be from the platform, to get them to put their credentials into a fake login site. The attacker could then use those credentials to log into the real account and steal money or commit a variety of downstream fraud. Users were also targeted by vishing attacks, where fraudsters would contact them by phone claiming to be from the platform asking for personal entails.

Ultimately, the company was unable to get a clear insight into whether real users or fraudsters with compromised accounts were coming to their site. This is evidenced by its 90% false positive rate and 80% false negative rate.

The Arkose Labs Solution

The company soon after engaged in a proof of concept with Arkose Labs. The Arkose Labs platform was implemented on the client's web and mobile app flows. Its robust detection engine was used to identify and classify bad traffic from good users and pass that information along to the client for remediation. Arkose Labs collected data that enhanced the client's models and gave them access to enhanced IP and device intelligence.

This increased insight into traffic patterns and access to additional data enabled the company to see the true extent to which these attacks were happening. Arkose Labs was able to detect when fraudulent account logins using phished, stolen credentials were happening and stopped them.

Arkose Labs was also used to identify and ensure that third-party aggregators are 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 ecosystem, such as customer support.

After this, the company abandoned plans to build an in-house solution and instead implemented the Arkose Labs platform.

Demonstrated Results

After implementing Arkose Labs, the client saw an almost complete reduction in compromised user accounts. 6.4 million token replay attacks were identified and stopped.

Arkose Labs also worked with the client for ongoing tuning of the platform to differentiate between legitimate traffic and attacks and respond to evolving traffic patterns. Arkose Labs demonstrated the ability to improve customer experience and lower overall attack volume, which was a key success metric for the client.

The Arkose Labs Advantage

Powerful Detection

Arkose Labs powerful detection engine accurately distinguishes between humans and malicious bots.

Constantly Learning Platform

The Arkose Labs solution continually evolves to adapt to new threats.

Managed Services

Arkose Labs works with businesses as true partners in fighting fraud.

Optimal User Experience

Good users are never blocked, which reduces false positives and helps the bottom line

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication", the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput.

Schedule Demo

demo@arkoselabs.com
arkoselabs.com