Arkose Labs

EBOOK

Your Holiday Guide to Fraud 2021

- Data-driven fraud insights
- 6 Lessons from 2020 Holiday Season
- Holiday Bot Attacks Data
- 4 Predictions for 2021

© 2021 Arkose Labs. All rights reserved.

This the Season to Be Jolly Prepared for Fraud

The holiday season is generally one of festivity, mirth, and merriment. Friends and family gather 'round dinner tables and living rooms to share tidings of gladness and joy and reflect on the year gone by.

Unfortunately, the holiday season is also a joyful time for fraudsters, but for all the wrong reasons. This is the time of year when fraud attacks rise to their most frequent and severe levels.

Expect fraud attacks to spike by at least 50 percent during the holiday season this year, if 2020 was any indication. This will potentially be even more of a spike for certain businesses, depending on the industry.

Holiday Season Attack Predictions

50% increase in overall attack volumes

2X credential stuffing attacks

Beyond Retail;
Financial services, media and gaming also in the crossfire

Account Security is Paramount

Account security is in the crosshairs during the holiday season. Fraudsters target both existing accounts — with credential stuffing and account takeover attacks — as well as fake new account registrations in order to take advantage of promotional offers and items, launch phishing attacks and scrape website information. Businesses must be prepared for the drastic increase in attacks targeting account security during this holiday season.

Holiday Season Account Security Attacks by the Numbers:

2.1 billion total attacks

50% of attacks from Asia

30% total attack rate

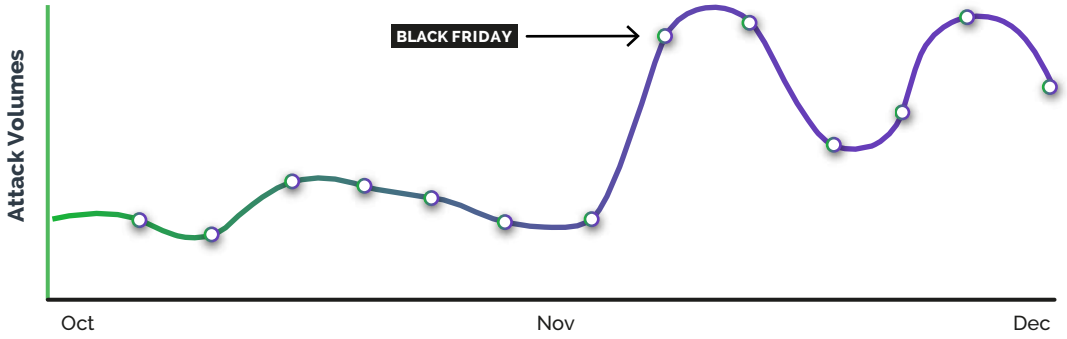
16% mobile attack rate

Top 6 Lessons from 2020 Holiday Season

1. Fraud attacks rise to their most frequent and severe levels across industries.
2. Fraudsters use higher digital traffic levels to "blend in" with good traffic.
3. Traffic spiked both the week before and during Black Friday, with attacks rising up to 56% higher.
4. These increases were not just in retail - Other industries saw three-to-five times the amount of attacks.
5. There was a heavy reliance on bots to carry out attacks, with 89% of all attacks being automated.
6. Mobile-based attacks also increased, from 15% to more than 17%.

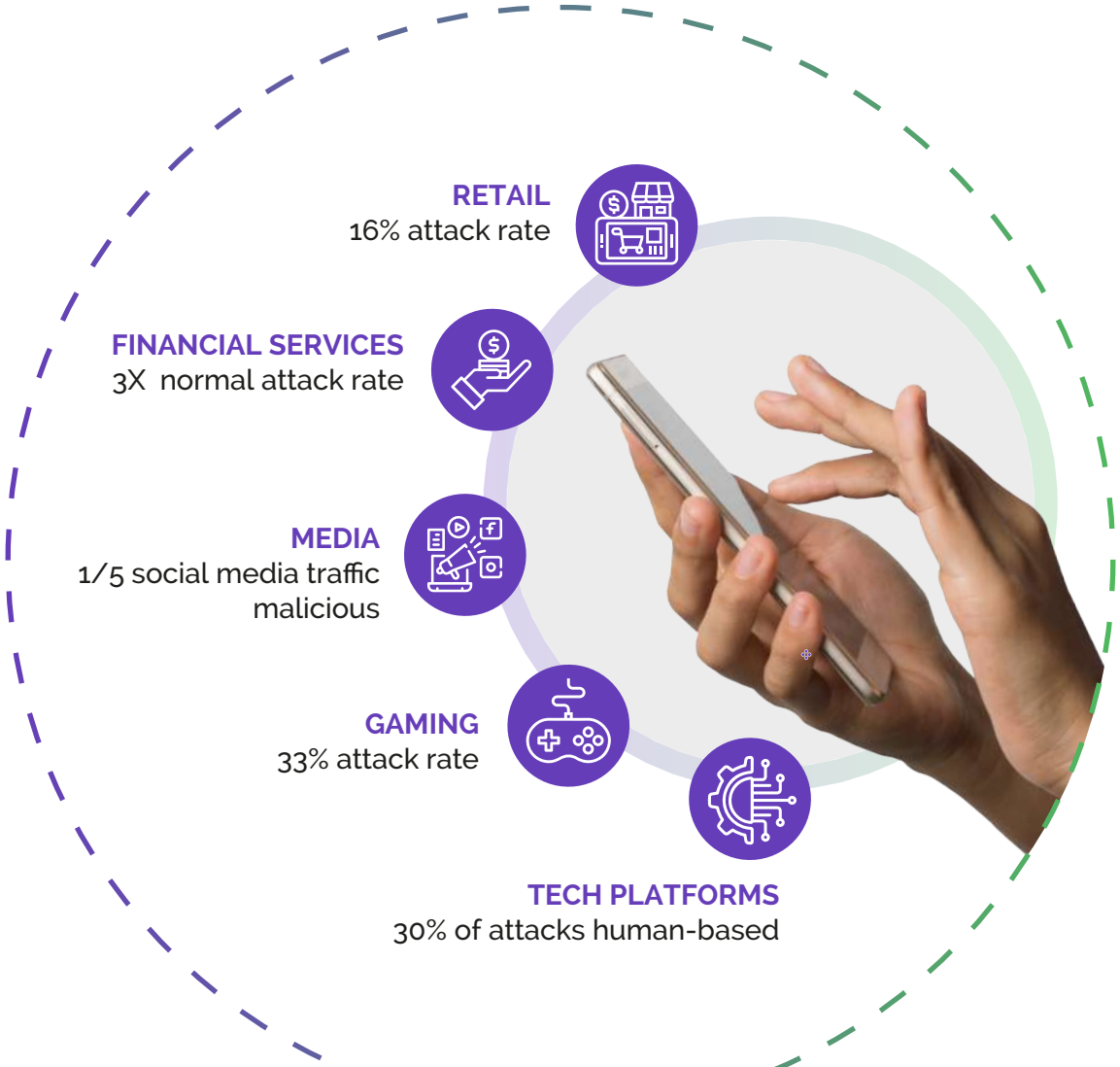
Q4 2020 Weekly Attack Volumes

Black Friday marks not only the beginning of the busiest shopping season of the year, but the busiest fraud season as well. Attacks targeting all industries spike up dramatically, with a sustained heightened level throughout the end of the year.



No, It's Not Just Retailers!

While ecommerce is obviously a high target during the holiday season, all industries are affected by an increase in fraud attacks. Fraudsters take advantage of the increased amount of digital traffic to all sites during this time and "blend in" with good users. With the increased amount of digital accounts being created during this period, ATO attacks increase dramatically. Fake new account fraud also rises during the holiday season, as fraudsters seek to take advantage of promotional items and offers meant to attract new customers.



Bots: Naughty or Nice?

Bots are very active during the holiday season. Many of them are "good bots" such as search engine crawlers, aggregator bots, marketing bots and bots that search websites looking for shopping comparisons or travel deals.

However, fraudsters also rely heavily on bots during this season to carry out attacks at scale. Credential stuffing, account takeovers, fake new account fraud, website scraping and many other attacks utilize automation at scale to be carried out efficiently and profitably.

Businesses need to prepare for an explosion in bot activity at this time of year. Sophisticated anti-bot defenses requires a mix of machine-learning powered detection and risk classification and the use of advanced, interactive challenges which cause bots to fail without disrupting user experience.

Holiday Bot Attacks at a Glance

- Automation accounts for 89% of all attacks
- Nearly 2 billion overall bot attacks
- North America and Europe have highest bot attack rate
- Gaming the most targeted industry by bot attacks
- Increase in hybrid human/bot attacks

2021 Predictions:
What to Expect this Holiday Season

Heightened attack volumes across industries

Last year attacks went up by 56% during the holiday season, and we would expect an even bigger increase this year. This was a trend that became pronounced last year. This will include companies typically not associated with Black Friday such as social media platforms, online dating, and financial services

Rise in Asia-based attacks

There was a massive uptick in attacks from Asia during last year's holiday period. This can be explained due to fraud attacks around Singles Day — an even bigger online shopping holiday than Black Friday. Asia accounted for more than 50% of all attacks last holiday season. Expect the same this year.

Rise in human-based attacks

We have seen an increase in human-based attacks during the holiday season. This shows that fraudsters are willing to put time and effort into attacking, beyond simple high-velocity bot attacks, when it comes to high-value targets. Last year saw 470 million human attacks during the holiday season; In ecommerce, humans account for 20% of all attacks.

Increase in gift card fraud

Fraudsters love targeting gift cards as they offer an instant route to monetization and are hard to track, much like cash. It provides quick money and generally an easy getaway. Gift card fraud attacks more than doubled in the holiday season 2020 compared to Q3; expect the same this year.

It's A Wonderful Time of the Year...
for Smarter Defenses

Businesses need a cost-efficient, long-term solution that goes beyond mere mitigation and adapts to evolving threats to create long-term fraud deterrence. They must adopt an integrated approach that can empower them to fight the onslaught of automated attacks with confidence and is cost-effective in the long run.

The holiday season is a prime time for fraud, and many businesses feel internal strains when fending off this onslaught of attacks. Fighting fraud may be more complicated than ever, but with the right approach and the right tools, you can stop the bad guys in their tracks while still maintaining a great digital experience for customers.

Determine Intent and Behavior

- Realtime 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

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.

Email: demo@arkoselabs.com

© 2021 Arkose Labs. All rights reserved.

Schedule Demo