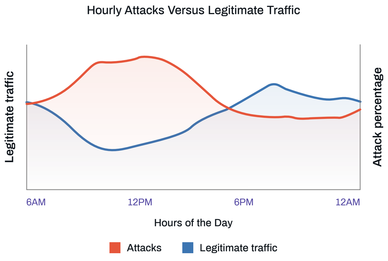
Arkose Labs

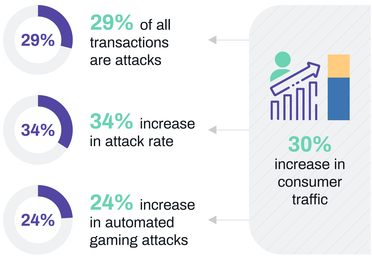
Gaming Insights from the Arkose Labs Network

30% Spike in Gaming Volume as Consumer Behavior Shifts During COVID-19

COVID-19 is a Catalyst for Gaming Fraud:

- Higher volumes throughout the day but peaking towards the evening and staying high into late night
- The attack volume remains consistent throughout the day, leading to a fluctuation in the attack rates





92% increase in total number of attacks

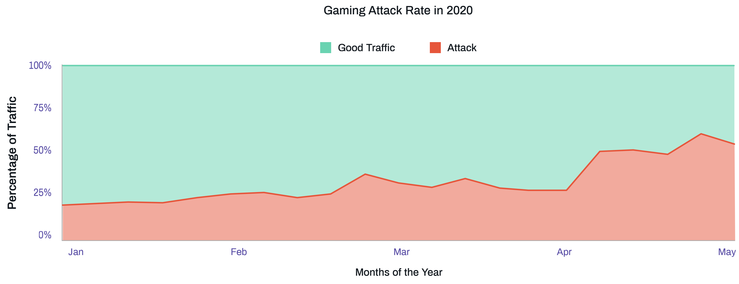
Logins most-attacked use case

40% attack rate from desktop traffic

Fraudsters have perfect conditions to carry out large-scale fraud:

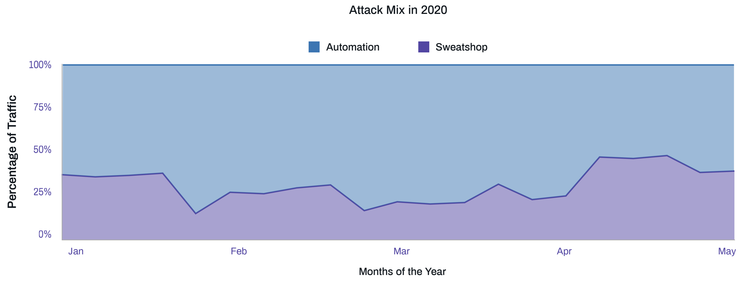
- Cost-effective human resources to carry out attacks
- Heightened incentive levels due to economic turmoil
- Plentiful fresh stolen user data
- High gaming volumes and user engagement across the globe
- Increasing digital activity across the globe
- Easy access to fraud toolkits

Rapid Growth of Traffic and Attacks:



Human-Driven Attack Trends During COVID-19 Crisis:

After an initial decline as the shelter in place orders went into effect, human-driven attacks have been increasing



Attack Trends Across Customer Touchpoints:

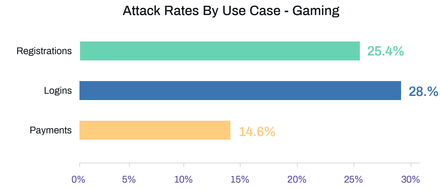
With the frenzy of fraudulent activity brought on by the COVID-19 global crisis, overall attack rates have gone up across most use cases

41% of in-game abuse is human-driven

In-game abuse: Attack levels are comparable to login, payment, and registration attack rates. These attacks could include in-game economy inflation, auction house scraping, gold/currency farming, and promo abuse.

46% rise in new account fraud

45% increase in login fraud



Download the full Q2 2020 Fraud and Abuse Report at www.arkoselabs.com