Arkose Labs | SPOTLIGHT

Real Money Trading

Online gaming is big business. Estimates peg the total value of the gaming industry at more than $150 billion as of 2019, and predicted to grow to $180 billion by 2021.[1] Within each online gaming metaverse also exist economies as intricate and complex as those in "the real world." Indeed, digital economies within video games are beginning to become a subject of interest for even trained economists.[2]

Of course, where there's money there will always be fraud. That's one reason why gaming was the most attacked industry in the first half of 2020, according to data from the Arkose Labs global network.

The Rise of In-game Economies

Some of this malicious activity is based around real money trading -- which is the selling of valuable in-game assets such as gold, items or even access to powerful characters themselves on so-called "gray market" forums. Obtaining such assets normally requires effort: they are the reward for players spending hours of in-game grinding, completing missions or other tasks. Attackers, however, will deploy bots at scale to perform the same repetitive actions over and over again in order to quickly accumulate in-game currency or valuable items or weapons. Since bot attacks are generally inexpensive and easy to deploy, the fraudsters can then turn around and sell these valuable assets on third party sites for much cheaper than they would normally go for on a company's official store or in-app purchase channel.

This leads to several wider negative effects as well, such as:

Harms Fair Play

Other players can simply purchase from fraudsters better items than what they've earned

Revenue Loss

When people buy farmed gold and items, instead of purchasing those through official company-provided channels, the gaming company has now lost out on potential revenue

ATO Attacks

Fraudsters are more motivated to compromise good user accounts to sell their valuable inventory

Bonus Abuse

Fraudsters create new accounts en masse in order to potentially obtain rare items that are meant as promotions to attract new customers.

[1]https://gamingshift.com/gaming-industry-worth/#:~:text=Right%20now%2C%20the%20gaming%20industry,15%20percent%20each%20consecutive%20year.
[2]https://medium.com/super-jump/why-online-gaming-matters-to-the-digital-economy-1e253c5de3b2

The Failings of Current Damage Limitation Tactics

Unfortunately for gaming companies, fighting this kind of malicious activity is difficult and often has unintended consequences that harm good players. Here's a few examples.

Banning of Users

Game developers will sometimes attempt to mass ban a large number of suspected bot accounts, events known as ban waves. However there are multiple problems with this approach. First, some good users will always invariably get caught in this net. As we know, gamers are not shy to voice their opinions on social media networks and forums such as reddit. So good users caught in ban waves will let the larger community know about their displeasure, which could cause negative brand connotations. Furthermore, ban waves usually occur only every few months, leaving large gaps of time where bots can run free.

Rolling Back Functionality

This is a drastic step that no gaming platform wants to take, but often is necessary due to rampant fraud. This can mean reducing or eliminating promotional items associated with opening new accounts, or scaling back special events or quests that are designed to reward players with rare inventory for completing them.

This has an effect not only on players but also game designers. Designers pride themselves on creating cool new features for players of the virtual world to use and interact with. Restricting functionality in the name of fighting fraud actually leads to less interesting and creative game worlds.

Fight Abuse Without Compromising the Gaming Experience

The Arkose Labs platform is uniquely positioned to help gaming companies stop real money trading and other malicious in-game abuse. Some of the highlights of the platform include:

- Protects traffic originating from games consoles, mobiles and desktop
- Protects consumer actions deep within games
- Eliminates 100% of bot activity in games
- On-brand authentication challenges
- Unique authentication inspired by gamification
- Roots out organized click farm activity

Arkose Labs is in a unique position to help address the issue of real money trading. It analyzes users to determine true internet, and can monitor activity from logged in users deep within gaming platforms. It remediates suspicious activity using in-band enforcement challenges, in a way that does not disrupt legitimate users.

This tackles abuse in real time, rather than relying on downstream banning. Bots are thwarted with interactive challenges that cannot be solved by machine vision technology. Malicious actors are shown increasingly difficult and complex challenges until they give up in frustration and leave. Arkose Labs works with gaming companies across the globe to fight all forms of in-game abuse, including auction house abuse, gold mining, inventory hoarding and more.

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com

Schedule Demo