Infinite Money Hackers

Detecting Suspicious Accounts using Classification Methods

Sandbox Challenge

Laurel Xiang, Michael Poma, Roshan Vemu, Evan Lau

Rationale

Player retention is a must when it comes to video games. However, fans have been deterred from continuing to play GTA Online due to the interference of hackers upon the gameplay.

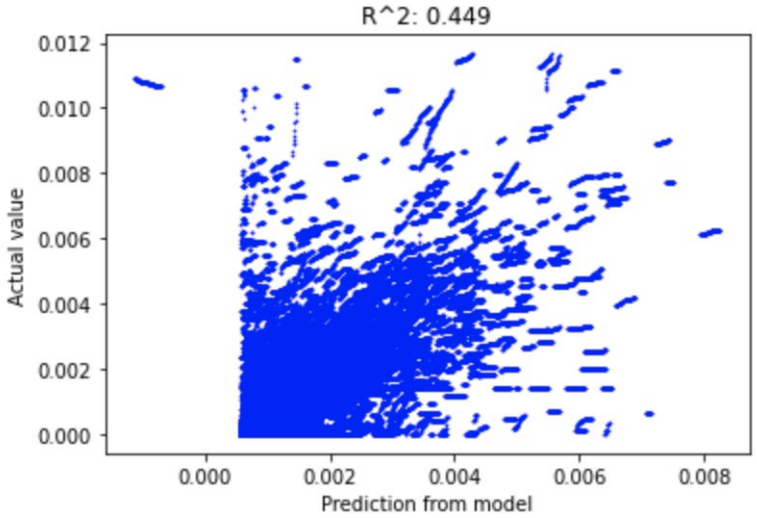
We've identified **suspicious players** based on their player activity and our personal experiences with the game.

Our main problem: the Hackers aren't labeled. So we had to figure out how to find them.

PHASE 1

Identify the **flagging metric**.

How can we capture **character rank** comparative to **total time played**?



PHASE 1

We computed **confidence intervals** for each login to determine the range where we expected the player's rank to fall between at the end of a session, with a **confidence level of 99%**.

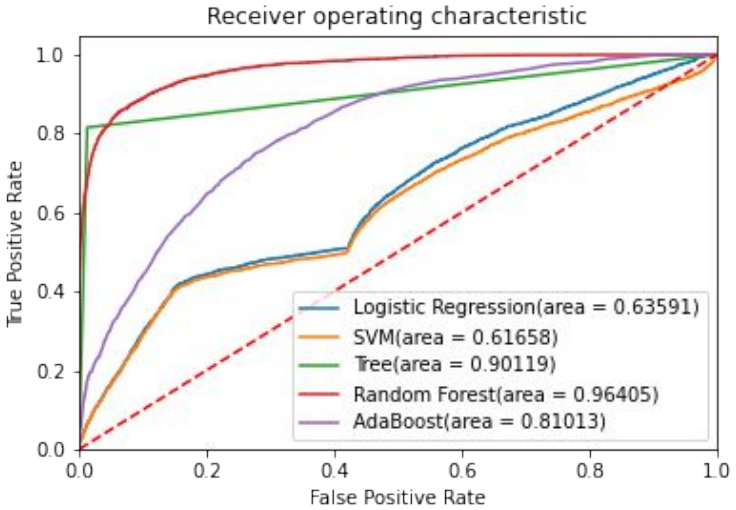
If the true rank exceeded the upper bound of the interval, we deemed this as ***suspicious behavior***.

We now found our **ground truth**: we artificially labeled the 522 "suspicious accounts" if they had exhibited the suspicious behavior described.

PHASE 2

We built **5 baseline classification** models to predict suspicious accounts that we labeled.

The **AdaBoost** model performed with an AUC of **0.810**, indicating that the model correctly classified between suspicious users and normal users **81.0%** of the time.



PHASE 3

Phase 3 was **scalability**.

The next steps of our approach would be to scale our best performing **AdaBoost** model from Phase 2.

Our **recommendations** to expand upon the project would be to specifically analyze the **behavior** of suspiciously **flagged accounts**, and to **increase the span of data** analyzed to draw more conclusions and determine a wider array of flagging metrics.