Detection of Hacker's Behavior in Gaming Software by using BOT Security

Rutuja Kaswa[1] Shreepad Kale[2] Kunal Mutha[3] Snehal Dagade[4]
[1,2,3,4]KJCOEMR Pune India

Abstract— Online games have many players they can purchase game money and online game have ecosystems from real money trading players get the money officially. The reason behind in raising gold farming groups is unofficial market of real money trading. Gold farming groups also called as GFGs. GFGs is a directly impact on real world and cyber. MMORPGs (massively multiplayer online role playing games) is one of the most interesting cyber economics reason is massive nature of game. GFGs detect gold farmers. GFG is technique to hide. That is concealing cyber money, front organization and changing trade pattern all those thing happen when online game providers ban GFGs. We build third to trace the gold farming groups and also analyze their behavior.

Key words: User Behavior Analysis, Sequence-Analysis, MMORPG, Game BOT, GFG

I. INTRODUCTION

When any two characters exchange items or game money, an in-game trade log is generated. In general, players exchange items for other items or money of an equivalent value.

However, in some cases, this exchange occurs even when the values of two items are quite different. For example, a user gives an item to other users as a present. However, GFG members give items or money to the character in a higher position to accumulate game items and money in the GFG. Accordingly, the in equivalent trades between GFG members are frequently observed. The free money and items are then sold to buyers who are normal users. To facilitate such process, the GFGs consist of three types of characters :gold farmers, merchants, and banking characters .Gold farmers repeatedly hunt (game) monsters and harvest craft materials to earn game money and items. Collected items and game money are delivered to merchant characters, and the merchant characters sell the items for game money. The game money from gold farmers and the money acquired through item trade by a merchant character flow to banking characters. Merchant characters receive the free money repeatedly and transfer the free money to other characters repeatedly.

The banking characters possess most of the game money in the GFG, and focus mainly on selling the game money for real money. The banking characters do not play the game, but focus on trading game money because they manage a large amount of it.

Hence, they have to keep their account safe from accusations by other users and blocking by the game company. When they are blocked, the game assets in the GFG are seized and written off from the market, causing significant damage to the GFG. Users who want to have high- level characters easily purchase game money for real money from these banking characters. Because of these illegal trades, the economic balance of the game collapses because, for example, an abnormal increase in the amount of game money and items causes inflation. In addition, gamers who buy goods with real money quickly achieve a high level. Those users who do not follow typical steps cause rapid consumption of the game content, which shortens the game lifecycle.

II. LITERATURE SURVEY:

A. Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games-

This paper reviews what we know so far about gold farming, seeking to provide the first systematic analysis of the sub-sector. It assembles available data at the spectral, enterprise and worker level. Five main analytical lenses are then applied. Economic analysis shows how exchange rate variations and scale economies do and do not impact gold farming; and the strong influence of information failure in the purchase of virtual items: known as "real-money trading". Analysis from the perspective of industrial sociology charts the commoditization and globalization of the sub-sector, while value chain models identify resource dependencies and power inequities. Enterprise analysis investigates enterprise entry, existence and progression, and outlines the competitive forces shaping the sub-sector's development; particularly threats. Developmental analysis investigates the impact of this sub-sector in macro and micro terms. Finally, there is a sociological analysis of the role played by perceptions and other social forces.

B. Crime Scene Re-investigation: A Postmortem Analysis of Game Account Stealers' Behaviors-

In this paper, we analyzed the action sequences of the account thieves and proposed a model to detect account thieves based on the analysis results. The proposed detection model is useful in detecting the theft of users even if the users do not perform security measures at the user-side. We analyzed transaction networks of the account thieves and analyzed their transaction characteristics and analyzed whether they are related to game bots.

C. Online Games and Security-

In this paper introduction to MMORPG security, we focus on bugs involving time and state. We can expect to see more of such bugs. as real-world software evolves to be-come more like game software.

D. The Ones That Got Away: False Negative Estimation Based Approaches for Gold Farmer Detection-

In this paper we address this gap in the literature by addressing the problem of false negative estimation for gold farmers in MMOs by employing the capture-recapture technique for false negative estimation and combine it with graph clustering techniques to determine ”hidden” gold farmers in social networks of farmers and normal players.

E. Multimodal game bot detection using user behavioral characteristics-

The aim of this study is to detect game bots in a massively multiplayer online role playing game (MMORPG). We observed the behavioral characteristics of game bots and found that they execute repetitive tasks associated with gold farming and real money trading. We propose a game bot detection method based on user behavioral characteristics. The method of this paper was applied to real data provided by a major MMORPG company. Detection accuracy rate increased to 96.06 % on the banned account list.

III. TECHNIQUES

Gold farmer detection methods have evolved over the years, and the literature on the problem can be classified into three generations of related works. The first generation of such methods is signature-based, and utilizes client-side bot detection such as antivirus programs or CAPTCHA-based techniques. However, the first generation of commercial products could be thwarted using techniques learned from reverse engineering. Also, methods using CAPTCHA are known to be user-unfriendly, and contribute to user annoyance.

Finally, solving CAPTCHA has generated a thriving business that uses mechanical Turks utilized by underground players. The second generation of methods focused on data mining techniques, and used server-side bot detection systems, which focused mainly on distinguishing between a bot and a benign player by analyzing server-side log files. Such techniques are widely used commercially and are coupled with logging techniques and various data mining algorithms for highly accurate bot detection. However, making a variant of an existing bot that can generate new behavioral patterns to thwart an existing detection technique is very easy and heavily utilized by gold farmers. Moreover, this method targets gold farmers individually. Companies have less insight of who belongs to the same group, and GFGs fight banning by continuously creating new gold farmers, making current banning efforts ineffective.

The third generation methods are a surgical strike policy. They can detect all industrialized GFGs by group assuming that members in a group have frequent interaction and abnormal patterns.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

IV. EXISTING SYSTEM

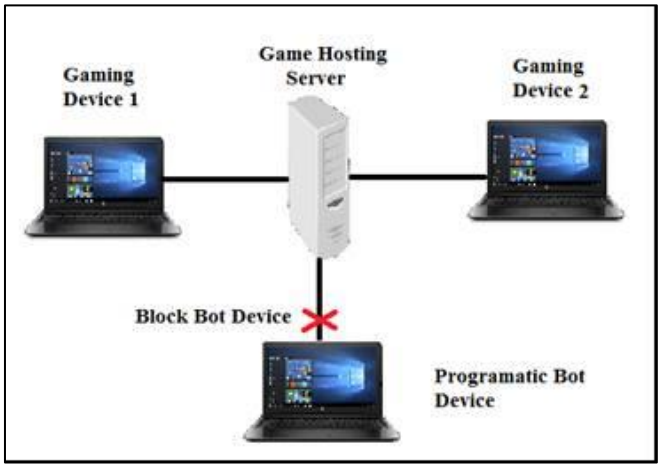

Fig. 1: System Design

V. PROPOSE SYSTEM

1) We write purchase module for any in app purchase game. In purchase module we design game purchase module which contain selling and buying criteria for the particular game.
2) Second task is to create bot which can play game automatically. For this we have to analyze whole software logic of the game. After understanding whole logic or algorithm of the game we are ready to create bot which can play game automatically.
3) Now the main task is to detect bot. we can detect bot by three scenarios which are as follows.
   - purchase module details
   - time period
   - location
   - If someone does selling only and cannot buy anything in any stage then it is suspicious then we declare that player as a bot and block.
   - If someone is playing game more than 8 hour or 24 hour then obviously it I it is suspicious so in this scenario we declare this player as a bot and block.
   - Last scenario is to find whether there is a group which can play game from different devices but location and IP are same. Then it will come under suspicious activity and we block that user.

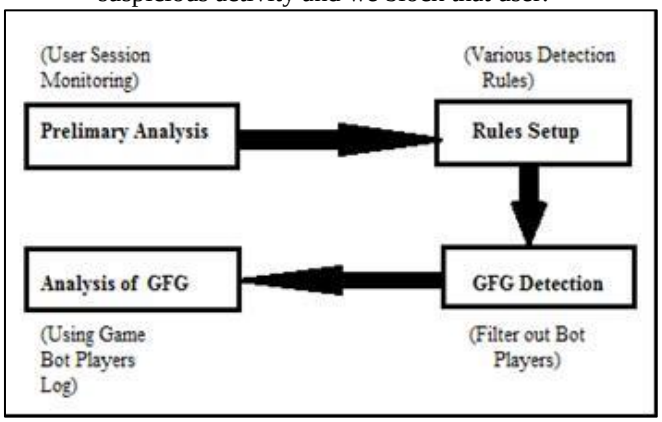

Fig. 1: Framework for Tracking GFGS

VI. CONCLUSION

We proposed a multimodal framework for detecting game bots in order to reduce damage to online game service providers and legitimate users. We observed the behavioral characteristics of game bots and found several unique and discriminative characteristics. We found that game bots execute repetitive tasks associated with earning unfair profits, they do not enjoy socializing with other players, are connected among themselves and exchange cyber assets with each other. Interestingly, some game bots use the mail function to collect cyber assets. We utilized those observations to build discriminative features. We evaluated the performance of the proposed framework based on highly accurate ground truth—resulting from the banning of bots by the game company. The results showed that the framework can achieve detection accuracy of 0.961. Nonetheless, we should consider that the banned list does not include every game bot.

The game company imposes a penalty point on an account that performs abnormal activities, and eventually blocks the account when its cumulative penalty score is quite high. Some game bots can evade the penalty scoring system of the game companies. Hence, the actions of a player are more important than whether the player is banned or not, and we concede that a player is a game bot when the player's actions are abnormal. We focused on those user behavioral patterns that reflect user status to interpret the false positive cases, and hypothesize that they are game bots not yet blocked, and false negative cases are human users occasionally employing a game bot. Although different from those in the banned list, they behave in the same pattern. We believe that our detection model is more robust by relying on multiple classes of features, and its analyses promise further interesting directions in understanding game bot and their detection.

REFERENCES

[1] Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games.
[2] Crime Scene Re-investigation: A Postmortem Analysis of Game Account Stealers' Behaviors.
[3] Online Games and Security.
[4] The Ones That Got Away: False Negative Estimation Based Approaches for Gold Farmer Detection.
[5] Multimodal game bot detection using user behavioral characteristics.

