МЕТОДЫ ОБНАРУЖЕНИЯ ИГРОВЫХ БОТОВ
Баланков Н.В. Email: Balankov6112@scientifictext.ru

Баланков Никита Валерьевич – студент,
кафедра информационных технологий,
Санкт-Петербургский государственный архитектурно-строительный университет,
г. Санкт-Петербург

Аннотация: *игровые боты – автоматизированные программы, которые приносят разработчикам игр как репутационные, так и экономические издержки. Боты дают одним игрокам преимущество над другими, чем провоцируют недовольство игроков и их отток из проекта. Именно поэтому проблема поиска ботов сейчас актуальна как никогда. Один из вопросов, который при этом встает: какому способу поиска отдать предпочтение? В данной статье было проведено сравнение различных методов автоматического обнаружения игровых ботов, выявлены их преимущества и недостатки.*
Ключевые слова: *игровые боты, поиск ботов, детекция на стороне клиента, детекция на стороне сервера, reCAPTCHA.*

GAME BOT DETECTION METHODS
Balankov N.V.

Balankov Nikita Valeriyevich – Student,
DEPARTMENT OF INFORMATION TECHNOLOGY,
SAINT-PETERSBURG STATE UNIVERSITY OF ARCHITECTURE AND CIVIL ENGINEERING,
SAINT-PETERSBURG

Abstract: *game bots are automated programs that cause both reputational and economic costs to game developers. Bots give some players an advantage over others, thereby provoking players' dissatisfaction and their exodus from the project. That is why the problem of finding bots is now more relevant than ever. One of the questions that arises at the same time: which search method should you give preference to? In this article, a comparison was made of various methods of automatic detection of game bots, their advantages and disadvantages were revealed.*
Keywords: *game bots, bot detection, client-side detection, server-side detection, CAPTCHA.*

УДК 004.925

Исследования по обнаружению игровых ботов можно разделить на три группы: на стороне сервера, на стороне клиента, на стороне сети.

Под клиентом понимается программа, которая работает на локальном компьютере, смартфоне или другом устройстве пользователя и осуществляет с другой программой (сервером) связь клиет-сервер. Поиск ботов на стороне клиента основан на сигнатуре, то есть при поиске отслеживаются аномалии, которые происходят на клиентской машине, при этом отправляются снимки экрана клиента на сервер. Для защиты от ботов и их обнаружения на стороне клиента используются разные способы, один из них – это встраивание тестов CAPTCHA [1]. Данные тесты строятся на разрыве возможностей людей и ботов, то есть на способности людей распознавать случайно искаженный текст или изображения. На смену CAPTHCA пришла ее усовершенствоанная версия reCAPTCHA, разработанная в 2007 году и продолжающая улучшаться до сих пор (см. Рис. 1).

Рис. 1. Современный вид теста reCAPTCHA

Однако, современные боты могут легко обойти подобный вид защиты используя встроенные нейронные сети. Кроме этого, поиск ботов на стороне клиента может вызывать проблемы в операционной системе пользователей, что доставляет им существенные неудобства. Исходя из вышесказанного, обнаружение игровых ботов на стороне клиента в настоящее время не является предпочтительным.

Поиск на стороне сети заключается в обнаружении различий в реакции игроков-людей и ботов при изменении сетевого трафика или сетевых пакетов. В статье [2] обнаружили, что боты демонстрируют более частые поступления пакетов на сервер и отправляют меньше информации, чем игроки-люди. Однако, самым существенным минусом обнаружения игровых ботов на стороне сети является вероятность перегрузки сети и увеличение задержки отклика сервера (ping), что значительно ухудшает игровой процесс.

Учитывая недостатки методов обнаружения игровых ботов на стороне клиента и на стороне сети, обнаружение игровых ботов на стороне сервера является наиболее востребованным методом обнаружения для игровых компаний. Этот метод берет данные журнала игроков, собранные с игрового сервера, и применяет методы интеллектуального анализа данных [3], поскольку игровые боты демонстрируют повторяющиеся модели поведения, отличающиеся от поведения игроков-людей. Следовательно, обнаружение игровых ботов на стороне сервера не вызывает никаких негативных эффектов.

Новейшие разработки для защиты от ботов представляют собой огромные фреймворки с хорошо настроенными сетями для высоской скорости реагирования на изменения в коде новых видов ботов. В статье [4] представлен один из таких фреймворков. Этот фреймворк производит обнаружение игровых ботов на стороне сервера на основе журнала игроков, что обеспечивает высокую точность и эффективность за счет заранее определенных алгоритмов поиска.

Современные решения, с недавних пор, стараются одновременно комбинировать кластеризацию, классификацию, механизмы выборки и сегментации и важнейший механизм – систему автоитерации. Система автоитерации позволяет переобучать хорошо настроенные сети с большей скоростью, предоставляя качественные новые наборы данных с неизвестными до этого момента ботами.

В переобучении сетей для поиска ботов также стали преобладать новые подходы, одним из них является трансферное обучение. Трансферное обучение предполагает использование уже накопленных знаний из прошлых задач для быстрого переобучения сети к новым задачам. Так постоянно получая наборы с новыми неизвестными ботами и передавая их на трансверное обучение, чтобы переобучить последние слои сети, можно значительно ускорить преспосабливаемость системы безопасности как к совершенно новым ботам, так и ботам, которые были известны ранее, но поменяли свои паттерны поведения.

Все эти механизмы в сумме позволяют быстро реагировать на изменения в поведениях ботов и обеспечивают отличную защиту, которая куда надежнее, чем рассмотренная ранее reCAPTCHA. При этом серверный подход обеспечивает решениям удобство как разработчикам, так и пользователям.

Разработчикам не требуется развертка дополнительных пакетов на компьютерах игроков, а игроки не испытывают дискомфорта от минусов, которые привносят рассмотренные ранее подходы.

Список литературы / References

1. *Philippe G., Nicolas D.* Preventing Bots from Playing Online Games // Comput. Entertain, 2005. № 3 (3). P. 31-37.
2. *Hilaire S., Kim H.C., Kim C.K.* How to deal with bot scum in MMORPGs? // IEEE Xplore, 2010. P. 1-6.
3. *YeonJun C., SungJune C., YongJun K.* Detecting and monitoring game bots based on large-scale user-behavior log data analysis in multiplayer online games // The Journal of Supercomputing, 2016. № 72 (9). P. 3572-3587.
4. *Jianrong T., Jiarong X., Linxia G.* NGUARD: A Game Bot Detection Framework for NetEase MMORPGs // ACM Digital Library. [Электронный ресурс], 2018. Режим доступа: https://www.kdd.org/kdd2018/accepted-papers/view/nguard-a-game-bot-detection-framework-for-netease-mmorpgs/ (дата обращения: 20.04.2021).