УДК 004.056.53

ИССЛЕДОВАНИЕ МЕТОДОВ И ПОДХОДОВ ДЛЯ ВЗЛОМА КОМПЬЮТЕРНЫХ ИГР И РАЗРАБОТКА МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ ИМ

Ткаченко С.А (ИТМО)
Научный руководитель – доцент, кандидат технических наук, Перл И.А. (ИТМО)

Введение. В современном мире компьютерные игры стали неотъемлемой частью жизни многих людей и важным социальным, экономическим и развлекательным сектором. Однако, с ростом популярности и прибыльности игровой индустрии, взломщики и злоумышленники всё чаще нацеливаются на незаконное получение преимуществ в игре, создание вредоносных программ и кражу цифровых активов. Исследование методов взлома компьютерных игр является необходимым для обеспечения безопасности игровых систем. С каждым годом взломщики становятся все более изощренными и их методы становятся более сложными. Поэтому, важно вести изучение этой области и разрабатывать новые механизмы противодействия, чтобы предотвращать взломы и обеспечивать безопасность компьютерных игр.

Основная часть. Программное обеспечение, разработанное с целью взлома игры принято называть читом. Чит – исполняемый код, который может быть введен в программу или запускаться параллельно для получения игроком дополнительных возможностей или преимуществ, таких как неограниченное здоровье, боеприпасы, невидимость и т.д.

В ходе исследований существующих читов была выявлена их классификация по методу взаимодействия с игровыми системами:

1) Внешние читы – функционируют в отдельном процессе, и если они скрыты от обнаружения другими способами, загружаясь в память иного процесса, они становятся скрытыми для первичного обнаружения.
2) Внутренние читы – встраиваются в игровой процесс посредством инжектора и после загрузки в игровую память вызывают точку входа кода в отдельном потоке.
3) Читы с сетевым анализом – перехватывают клиентский и серверный интернет трафик, получая необходимую информацию и модифицируя входные или выходные пакеты.

Одним из эффективных методов противодействия взлому это наличие анти-чита, и полученная классификация позволяет понять основные принципы и подходы при разработке защитного программного обеспечения. Для исполнения своего предназначения внешний и внутренний чит должен модифицировать память компьютерной игры, а значит конечная цель у них одинаковая, отличается лишь способ получения доступа. Однако только получения доступа к памяти будет недостаточно, необходимы также специальные паттерны памяти для внесения корректных, с точки зрения чита, преобразований данных. Поэтому защитная система должна отслеживать несанкционированные изменения в памяти и принимать соответствующие меры к игрокам, использующих вредоносные программы.

Для борьбы с изменением сетевого трафика сервер и клиент могут использовать криптографические методы шифрования, что усложнит разработку чита, и даже может сделать невозможным модификацию пакетов данных.

Следующий метод для противодействию взлому игры – это исключения возможности получения данных для изменения или фильтрация получаемых от игрока данных. К примеру, вычисление скорости игровых аватаров, с заранее известным максимумом, или симуляция происходящего и задержкой отправки координат других игроков, находящихся вне зоны прямой видимости. Данные меры необходимо предпринять на стадии разработки и требуют определенных трудозатрат, но могут стать хорошей защитой от взлома кода игры.

Кроме описанных выше методов, применяется и желание других игроков избавится от нечестных соперников. Для этого можно добавить систему жалоб и записи игр. При подозрении на использование чита пользователи могут отправлять жалобы, которые затем

будут рассмотрены администраторами.

Выводы. Проведено исследование и анализ подходов ко взлому игр и выработаны механизмы для противодействия им. Полученные данные об методах воздействия на игровые процессы и жизненном цикле чит программ будут использован для создания собственной анти-чит системы

Список использованных источников:

1. Защита от читеров на примерах для Unity [Электронный ресурс]. Режим доступа: https://habr.com/ru/articles/589899/ свободный (20.01.2024)
2. Реверс-инжиниринг популярного античита BattlEye [Электронный ресурс]. Режим доступа: https://habr.com/ru/articles/483068//, свободный (15.01.2024)