Анализируемая модификация игры, доступная в TerjeBruoygard/TerjeMods, следует модели разработки, установленной Bohemia Interactive, и использует язык Enforce Script, предоставленный разработчиком игрового движка. Цель мода — позволить участникам одной группы видеть друг друга в игровом интерфейсе и на карте посредством отображения визуальных маркеров.

Контекст и принцип работы

Анализируемая модификация — **Terje Party Mod** для игры DayZ, предназначенная для создания групп (*party*) между игроками внутри игрового мира. Наблюдаемый механизм работы следует следующему сценарию:

- Игрок **A** взаимодействует (клавиша **F**) с Игроком **B**, отправляя приглашение в группу;
- Игрок **B** взаимодействует (клавиша **F**) с Игроком **A**, принимая приглашение;
- Группа создаётся, и игроки начинают видеть друг друга через маркеры в интерфейсе и на карте.

Наблюдение аномального поведения

В ходе эмпирических тестов было выявлено неконсистентное поведение после **полной переустановки операционной системы**, с удалением всех локальных папок и данных. В наблюдаемой ситуации:

- Анализируемый игрок **больше не видел группу**, как будто не состоял в ней;
- Другой игрок по-прежнему **видел первого игрока как участника группы**;
- Со стороны сервера не было выполнено явного действия по удалению группы.

Эта асимметрия привела к первоначальной гипотезе о том, что **информация о группе не полностью хранится или валидируется на сервере**, а зависит от данных, сохраняемых локально на клиенте.

Техническое исследование

Мониторинг файлов

Процесс DayZ отслеживался во время создания группы с использованием инструментов системного мониторинга (Microsoft Task Manager / Resource Monitor / Process Explorer) с целью выявления обращений к релевантным локальным файлам.

В результате был выявлен повторяющийся доступ к следующему файлу:

`TerjeParty.dat`

Этот файл открывался и изменялся в момент создания или обновления группы.

Анализ файла

Файл `TerjeParty.dat` был проанализирован с использованием **шестнадцатеричного редактора**, при этом после создания группы была обнаружена устойчивая бинарная структура, указывающая на хранение локальных конфигурационных данных.

Структура файла

Формат файла следует детерминированной структуре:

- **Начальный заголовок (4 байта, int32, little-endian):**
  - Представляет общее количество GUID, хранящихся в файле.
- **Последовательные записи для каждого GUID:**
  - 4 байта (int32, little-endian), указывающие размер **N** строки GUID;
  - **N байт**, содержащие GUID в формате **UTF-8**, без дополнительного терминатора.

Каждый GUID представляет собой идентификатор игрока и хранится в виде **строки Base64 (URL-safe)**, а не как фиксированное бинарное значение.

Наблюдаемое поведение записи заключается в простом **добавлении новых записей в конец файла**, при этом требуется лишь обновить начальный счётчик GUID для сохранения целостности формата.

Наблюдаемые свойства

- Структура файла **простая, последовательная и детерминированная**, что облегчает ручной разбор;
- Структура вида `[количество → размер → строка]` позволяет выполнять **прямые вставки и модификации**, при условии корректировки заголовка;

- Данные хранятся локально в читаемом формате (Base64), **без встроенного шифрования или проверки целостности**.

Эти характеристики объясняют как исчезновение групп после удаления локальных данных, так и возможность их ручного восстановления.

Исследование структуры

В ходе анализа внутри `TerjeParty.dat` удалось определить:

- Общее количество сохранённых идентификаторов;
- Полный список GUID, соответствующих участникам группы.

Было установлено, что GUID, используемый в DayZ, формируется на основе **SteamID** игрока через следующий процесс:

`SteamID → SHA-256 → Base64 (URL-safe) → GUID`

Наблюдаемый пример:

- SteamID: `76561198012345678`
- SHA-256: `c991f9c7f37b12d7b3deddeb607ab338af88f4cbd253171c02cce3b...`
- GUID (Base64 URL-safe): `yZH5x_N7Etez3t3rYHqzOK-I9MvSUxccAszjtPnnRlc`

Эксплойт / Доказательство концепции

На основе полного понимания структуры файла `TerjeParty.dat` стало возможным:

- Вручную записывать GUID в файл;
- Создавать **кастомные группы локально** без легитимного внутриигрового взаимодействия;
- Добавлять игроков в группу **зная только их SteamID**.

После ручной модификации файла игра распознавала добавленных игроков как действительных участников группы, что демонстрирует отсутствие **надёжной серверной валидации состава группы**.

Доказательство концепции и проведённые эксперименты задокументированы по адресу:

https://github.com/PSalleSDev/TerjeExp

Примечание автора

Данный документ подготовлен с **исключительно техническим, академическим и нейтральным характером** и имеет единственную цель — **анализ и документирование наблюдаемых поведенческих особенностей** в системах рассматриваемой модификации. Подготовка данного материала **не преследует коммерческих целей** и не направлена на неправомерное раскрытие информации, дискредитацию или нанесение ущерба инициативе или её разработчикам.

Основная мотивация данной работы — **содействовать укреплению мода**, поддерживая его дальнейшее развитие и обеспечение более **безопасной, надёжной и стабильной** среды для всех участников.

Публикация представленных наблюдений и анализа осуществляется в рамках **обмена техническими знаниями**, с намерением помочь разработчикам мода выявить точки для улучшения, минимизировать риски и усовершенствовать применяемые практики. Исходной позицией является убеждение, что техническая прозрачность и конструктивный диалог являются фундаментальными инструментами устойчивого развития общественных и коллаборативных проектов.

Данный документ следует рассматривать как **позитивный и конструктивный вклад**, направленный на продвижение лучших практик безопасности и обеспечение качественного игрового опыта для сообщества, основанного на **взаимном доверии** между разработчиками и игроками.