# Forensics-10-1

## Вредоносный мод‑пак

### Условие задачи

На популярном форуме распространялся «оптимизированный» мод‑пак для увеличения FPS. После его установки у игроков начали пропадать вещи из сундуков. В наличии архив с модами modpack.zip, клиентские логи пострадавшего client\_logs.txt и каталог с установленными модами mods\_folder/. Нужно найти вредоносный мод и выяснить его функционал.

### Что требуется найти

Флаг №1 — название вредоносного мода. Флаг №2 — порт, на который мод отправляет данные. Флаг №3 — команду, которую мод выполняет скрытно от игрока.

### Используемые инструменты

unzip, grep, strings, find, jadx или другой Java‑декомпилятор.

### Анализ и решение

Вредоносные моды имеют характерные признаки: нестандартные имена классов (Backdoor, Client, Stealer) и часто больше по размеру, чем обычные. Перебираем все JAR‑файлы в каталоге mods\_folder/ и ищем наличие классов, связанных с бэкдором. Команда unzip -l для каждого файла и поиск слова backdoor выявляет мод OptiFPS-1.19.2.jar. Этот файл подозрительно большой и маскируется под оптимизатор FPS. Его имя становится первым флагом.

Чтобы определить порт, распаковываем найденный JAR и ищем в исходниках упоминания соединений. В файле BackdoorClient.java встречается строка SERVER\_PORT = 25566. Этот порт использует мод для связи с удалённым сервером, что является вторым флагом.

В логах клиента фиксируются скрытные команды. Извлекаем строки из client\_logs.txt и ищем записи, связанные с выполнением команд: strings client\_logs.txt | grep -B2 -E "command|execute|silent". В одном из фрагментов появляется запись [HIDDEN] Command executed: /give @p diamond 64. По условию в ответе нужно удалить слеш и заменить пробелы на подчёркивания. Таким образом, третий флаг будет give\_@p\_diamond\_64.

### Итог

| Флаг | Значение |
| --- | --- |
| №1 | OptiFPS-1.19.2.jar |
| №2 | 25566 |
| №3 | give\_@p\_diamond\_64 |