# Forensics-9-1

## Зараженный лаунчер Pinecraft

### Условие задачи

Несколько игроков жаловались, что после установки «улучшенного» лаунчера ZLauncher‑Premium их аккаунты были взломаны. В нашем распоряжении установочный файл лаунчера zlauncher-premium.jar и дамп процесса launcher\_process.dmp. Необходимо найти вредоносный код и определить, какие данные и куда утекают.

### Что требуется найти

Флаг №1 — MD5‑хеш вредоносного файла. Флаг №2 — URL, куда отправляются пароли игроков. Флаг №3 — ключ для расшифровки логов лаунчера.

### Используемые инструменты

unzip, jar, md5sum, strings, grep, xxd.

### Анализ и решение

Чтобы выделить вредоносный компонент, распаковываем zlauncher-premium.jar как ZIP‑архив с помощью unzip. Внутри находится набор файлов .class. Среди них обнаруживается класс Stealer.class, название которого явно указывает на вредоносную функцию. Вычисляем MD5‑хеш этого файла с помощью md5sum и получаем значение 9b7dab9e88563c2ea2211165a2a463c9 — это и есть первый флаг.

Для обнаружения канала утечки ищем строки с сетевыми адресами в дампе памяти: strings launcher\_process.dmp | grep http. Среди результатов присутствует HTTP‑запрос POST http://steal.darkmc.ru/collect, который указывает на URL, куда отправляются похищенные пароли. Этот адрес и является вторым флагом.

Третий флаг — ключ для расшифровки логов — также можно извлечь из дампа памяти. Поиск по ключевым словам (strings launcher\_process.dmp | grep -i key) показывает строку XOR\_KEY = "MC2026". Это значение используется для XOR‑шифрования логов, и его нужно сообщить как третий флаг.

### Итог

| Флаг | Значение |
| --- | --- |
| №1 | 9b7dab9e88563c2ea2211165a2a463c9 |
| №2 | http://steal.darkmc.ru/collect |
| №3 | MC2026 |