# Forensics-11-2

## Свиноплагин

### Условие задачи

На сервере Pinecraft обнаружен подозрительный плагин EconomyPlus.jar. После его установки администраторы заметили утечки данных и странную сетевую активность. В наличии сам плагин и дамп сетевого трафика infected\_traffic.pcap. Нужно определить порт C&C‑сервера, название функции кражи данных и украденный пароль администратора.

### Что требуется найти

Флаг №1 — порт C&C‑сервера. Флаг №2 — название функции кражи данных. Флаг №3 — украденный пароль администратора.

### Используемые инструменты

unzip, grep, декомпилятор Java (jadx, JD‑GUI, CFR), Wireshark, XOR‑дешифровка.

### Анализ и решение

Внутри JAR‑файла обычно содержатся жёстко прописанные адреса сервера управления. Распаковываем EconomyPlus.jar и ищем строки с http: grep -r "http" .. В классе Backdoor.class обнаруживается URL http://badserver.tk:8080/panel. Нас интересует только порт, поэтому первым флагом является 8080.

Обфусцированные плагины маскируют имена методов. Декомпиляция плагина показывает массив байтов OBF\_METHOD и строку KEY = "minecraft". Функция d() выполняет XOR‑дешифровку и превращает массив в строку. Сопоставляя байты с символами ключа, получаем exfiltrateData. Это имя функции, отвечающей за кражу данных, и второй флаг.

В infected\_traffic.pcap фиксируются HTTP‑запросы с украденными данными. Открыв дамп в Wireshark и выбрав POST‑запрос, видим JSON:

{  
 "username": "AdminSteve",  
 "password": "1e1c1e001121040506081d5f575051",  
 "server": "pinecraft"  
}

Пароль представлен в виде hex‑строки. В плагине функция obfuscate() описана как XOR каждого байта с ключом minecraft и последующее кодирование в hex. Преобразуем hex‑строку обратно в байты и применяем XOR с повторяющимся ключом. Результат — SuperSecret123!, что является третьим флагом.

### Итог

| Флаг | Значение |
| --- | --- |
| №1 | 8080 |
| №2 | exfiltrateData |
| №3 | SuperSecret123! |