# Кейс. Расследование атаки: ненадежный VPN и забытые УЗ бывших сотрудников

›› Расследование и реагирование

## ЖЕРТВА АТАК

Государственная компания

Последствие атаки:
Шпионаж, компрометация инфраструктуры

Уровень атак:
Продвинутые / Целенаправленные

APT-группировка:
Shedding Zmiy

Способ проникновения:
Скомпрометированные учетные данные

## ДЕТАЛИ АТАКИ

6 месяцев атакующие находились в инфраструктуре, использовали ВПО для экспорта данных и скриншотов экрана.

Учетные записи уволенных сотрудников не были выведены из эксплуатации, чем и воспользовались атакующие

Компрометации стандартной УЗ в PostgreSQL, у которой был установлен ненадежный пароль

При самостоятельном реагировании были совершены достаточно распространенные ошибки:

- Пропуск уникальных файлов вредоносного ПО, которое не может быть обнаружено антивирусами из-за отсутствия сигнатуры.
- Не был обнаружен источник компрометации, в данном случае VPN-сервер

## СХЕМА ХРОНОЛОГИИ АТАКИ

Указана на следующем слайде

SOLAR | 4RAYS by SOLAR

## РЕШЕНИЕ

Расследование и реагирование на инциденты (DFIR)

## ДЕТАЛИ РАССЛЕДОВАНИЯ

[01] После получения доступа к VPN в апреле 2025 года атакующие скомпрометировали сервер PostgreSQL

[02] Обнаружили следы удаленного выполнения команд в системе с использованием легитимной функциональности самой БД

[03] Для закрепления в системе атакующие разместили утилиту gs-netcat, закрепив ее в файлах «.profile» и «cron» УЗ в PostgreSQL.

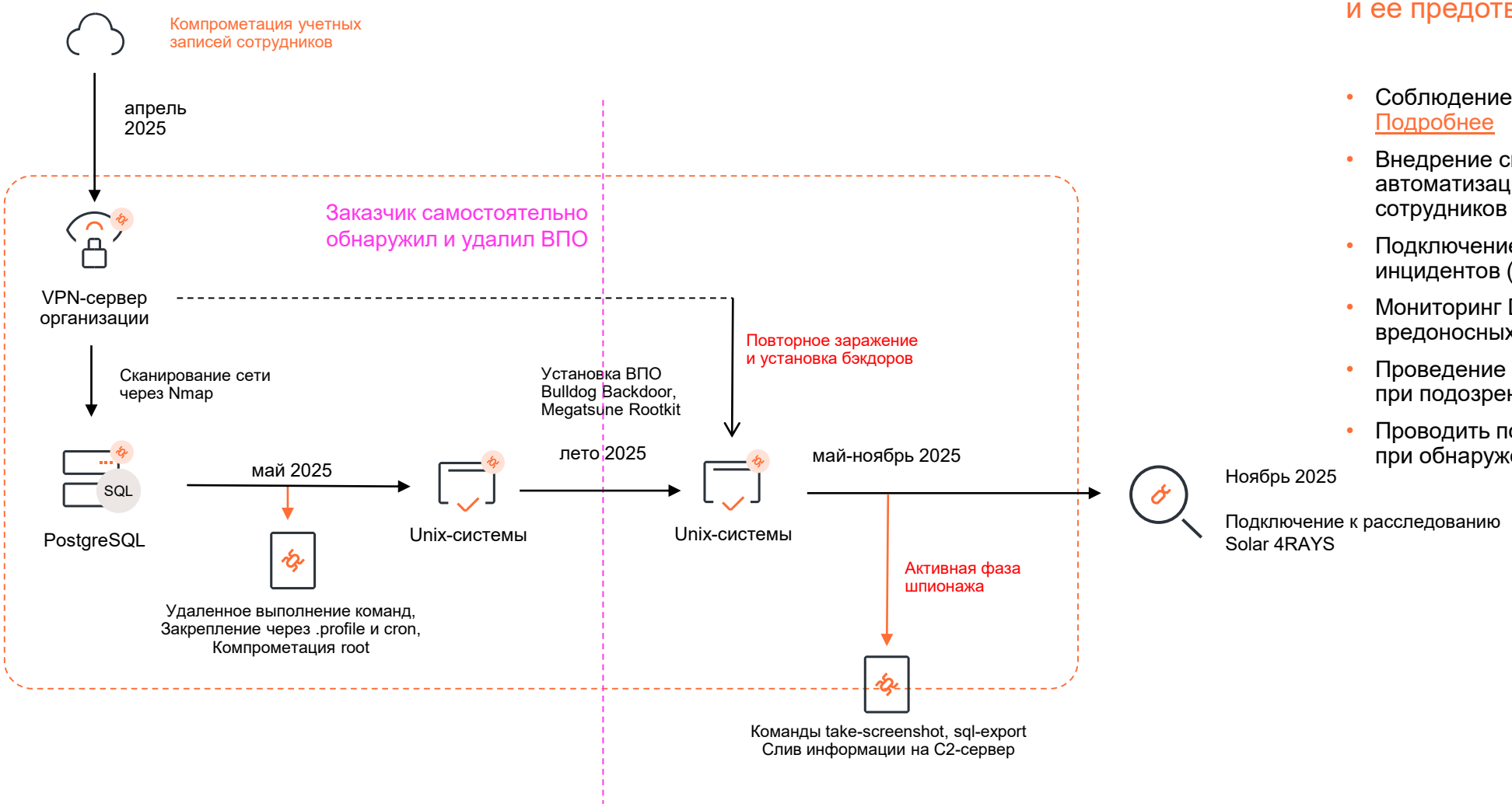
[04] Дополнительные детали:
- скомпрометировано несколько десятков Unix-систем
- через несколько дней у атакующих появилось множество учетных данных (в том числе root)
- атакующие с новыми учетными данными продолжали подключаться напрямую через VPN и длительное время не использовали размещенные в системах бэкдоры

Технические детали расследования доступны в статье блога Solar 4RAYS

# Кейс. Расследование атаки: ненадежный VPN и забытые УЗ бывших сотрудников

›› Расследование и реагирование

## ХРОНОЛОГИЯ АТАКИ




## РЕКОМЕНДАЦИИ по возможной остановки атаки и ее предотвращению

- Соблюдение базовых правил кибергигиены Подробнее
- Внедрение системы класса IdM для автоматизации блокировки уволенных сотрудников
- Подключение к мониторингу и анализу инцидентов (SOC), потокам данных TI Feeds
- Мониторинг DNS-трафика, блокировка вредоносных и фишинговых доменов
- Проведение Compromise Assessment при подозрении на атаку
- Проводить полноценное DFIR-расследование при обнаружение вредоносной активности