Даниэль Клюев

Эксперт в области извлечения и
анализа данных из персональных компьютеров

DFIR: расследование и предотвращение инцидентов

Оксиджен софтвер

ВЕДУЩИЙ РОССИЙСКИЙ РАЗРАБОТЧИК В ОБЛАСТИ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Наша миссия

Мы помогаем обществу становиться безопаснее. Решениями нашей компании в вопросах извлечения и исследования данных из мобильных устройств, облачных сервисов и рабочих станций пользуются правоохранительные органы, государственные учреждения, а также службы безопасности коммерческих организаций России и стран СНГ.

22 года на рынке

Наши продукты

Мобильный Криминалист Эксперт

Для проведения комплексной цифровой экспертизы данных из мобильных устройств, облачных сервисов и персональных компьютеров

Мобильный Криминалист Enterprise

Для расследования корпоративных инцидентов и проведения аудита путем извлечения данных из рабочих станций, мобильных устройств и облачных сервисов

Мобильный Криминалист Десктоп

Для извлечения и анализа данных из рабочих станций на Windows, macOS, GNU/Linux или образов с файловой системой NTFS

Мобильный Криминалист Экспертный Центр

Разновидность лицензии продукта «МК Эксперт» для одновременной работы с программой нескольких сотен человек

КЕЙСЫ, КОТОРЫЕ ЧАЩЕ ВСЕГО РАССЛЕДУЮТ С ПРИМЕНЕНИЕМ ИНСТРУМЕНТОВ DFIR (DIGITAL FORENSICS & INCIDENT RESPONSE)

ФИШИНГ

ВРЕДОНОСНОЕ ПО

МОШЕННИЧЕСТВО

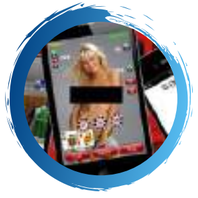
НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ АКТИВОВ КОМПАНИИ/НАРУШЕНИЕ ВНУТРЕННИХ ПОЛИТИК

УТЕЧКА ДАННЫХ

E-DISCOVERY

ПРОГРАММЫ-ВЫМОГАТЕЛИ

УВОЛЬНЕНИЕ СОТРУДНИКА С РАБОТЫ



ЗАПРЕЩЕННЫЕ ПРИЛОЖЕНИЯ

ХАРАССМЕНТ

ИСТОРИЯ ИНЦИДЕНТА

Оксиджен софтвер

У КОМПАНИИ НАЧАЛИСЬ ПРОБЛЕМЫ

За месяц потеряно несколько потенциальных клиентов в самом финале переговоров

КОНКУРЕНТЫ ЧТО-ТО ЗНАЮТ...

Один из постоянных клиентов сообщает, что на них вышли конкуренты и предложили более выгодные условия

КАЖЕТСЯ, КТО-ТО «СЛИЛ» ИНФОРМАЦИЮ

По характеру происходящего понятно, что конкуренты получили доступ к внутренним документам компании

«MK Enterprise»
АГЕНТСКИЙ РЕЖИМ

Оксиджен софтвер

«MK Enterprise»
АГЕНТСКИЙ РЕЖИМ

Оксиджен софтвер

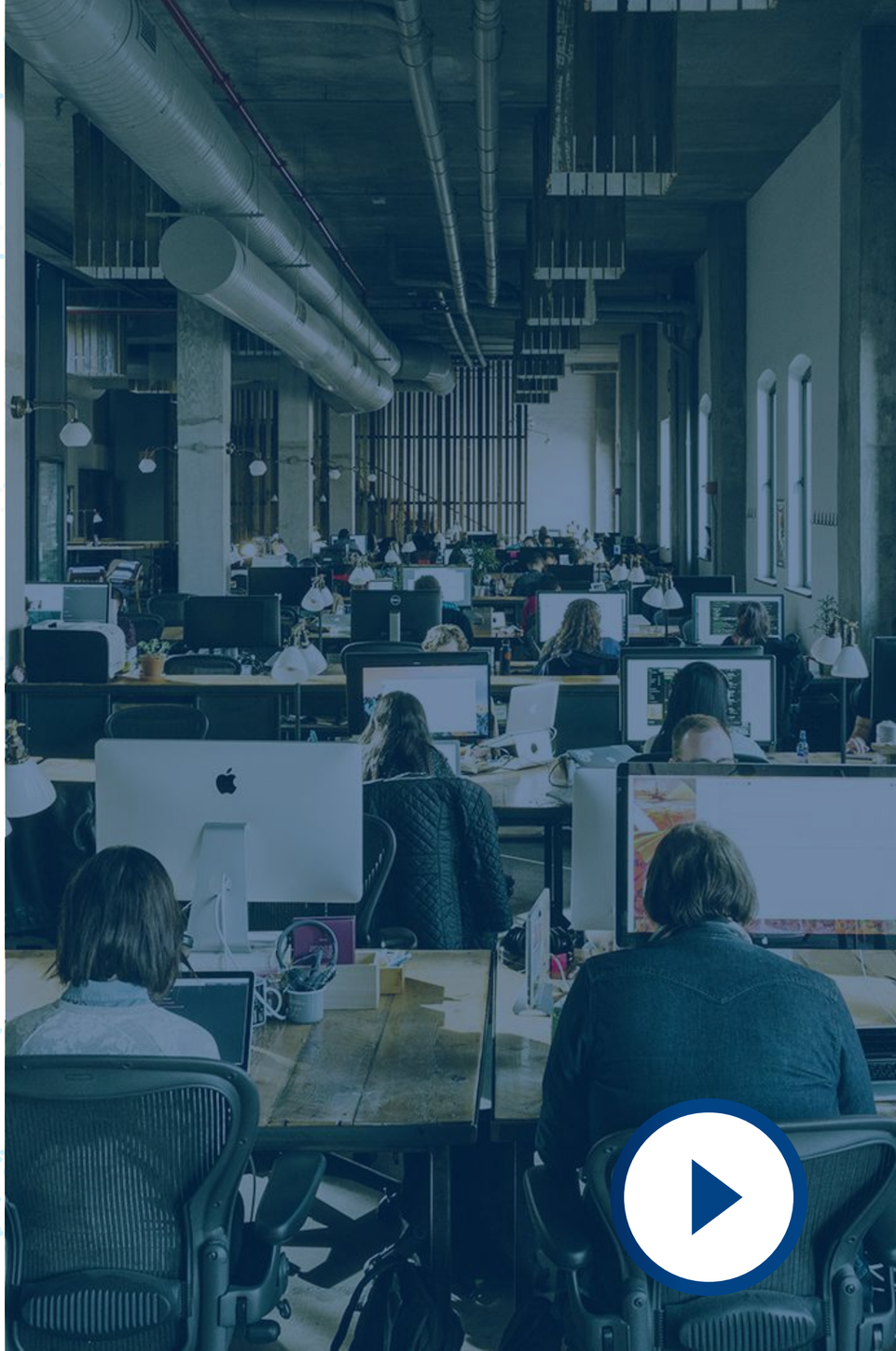
ПОИСК И СБОР ДАННЫХ

СОЗДАНИЕ ПРОФИЛЯ ПОИСКА

СОХРАНЕНИЕ ПРОФИЛЯ ПОИСКА

1 Этапы расследования

Необходимо установить, на каких рабочих станциях сети хранились документы, слитые конкурентам, или остались их следы



2 Этапы расследования

По итогам анализа рабочих станций сети, найдено 3 объекта дальнейшего исследования:

ПК главного бухгалтера Петровой Марии

ПК менеджера по продажам Петрова Игоря

ПК помощника бухгалтера Копыловой Анны

3 Этапы расследования

Проводим полный анализ трех целевых систем, чтобы определить какая из них была задействована в возможной утечке данных

4 Этапы расследования

Проводим анализ целевых систем

Находим мелкие нарушения, не доказывающие чью-либо вину

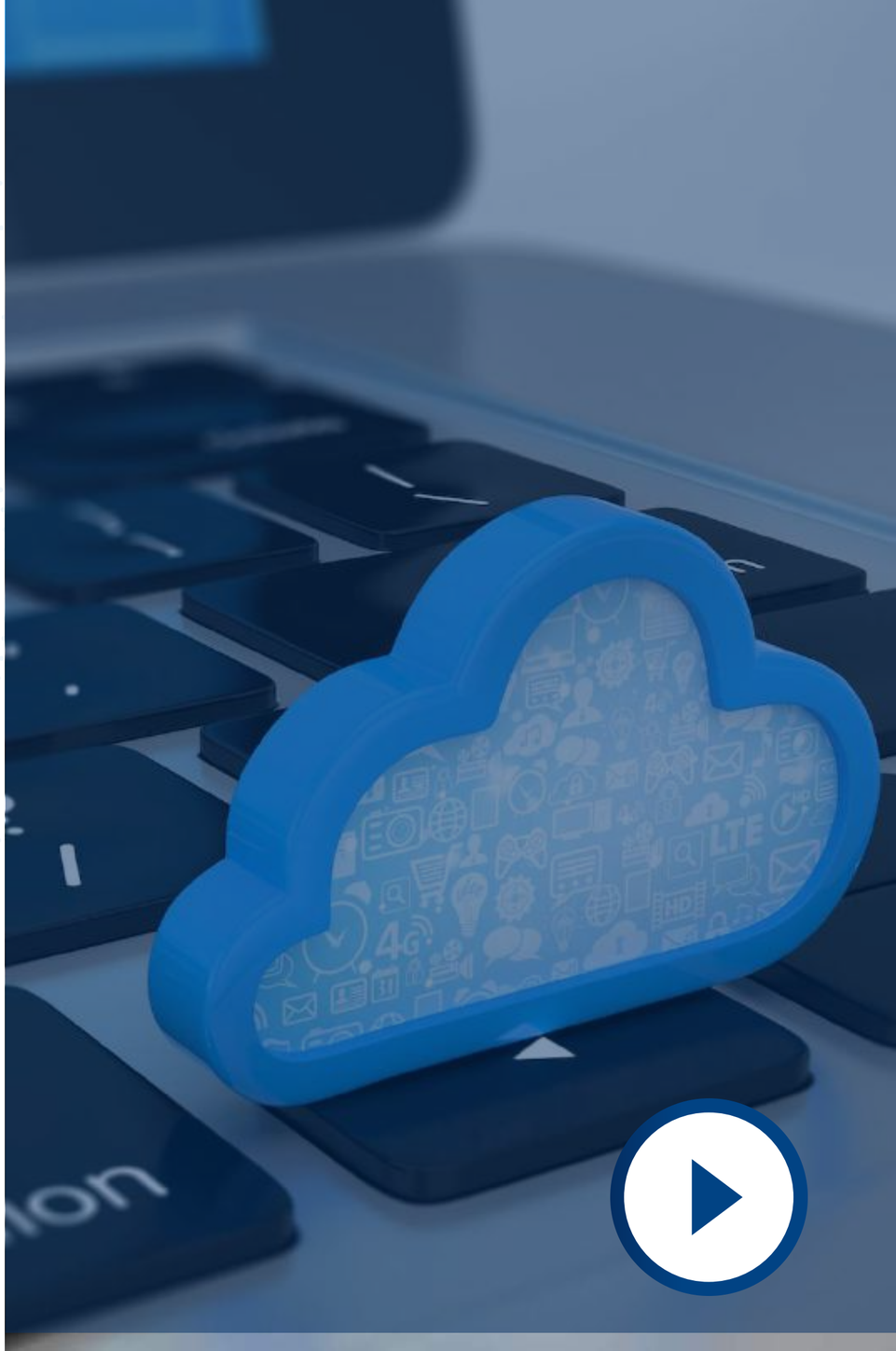
Обнаруживаем, что Мария Петрова передала документы Копыловой Анне

5 Этапы расследования

Проводим анализ целевых систем:

У Петрова Игоря обнаруживаем следы копирования файлов на внешний носитель

Проводим новый поиск по всей сети по следам с ПК Петрова Игоря



6 Этапы расследования

Проводим анализ целевых систем:

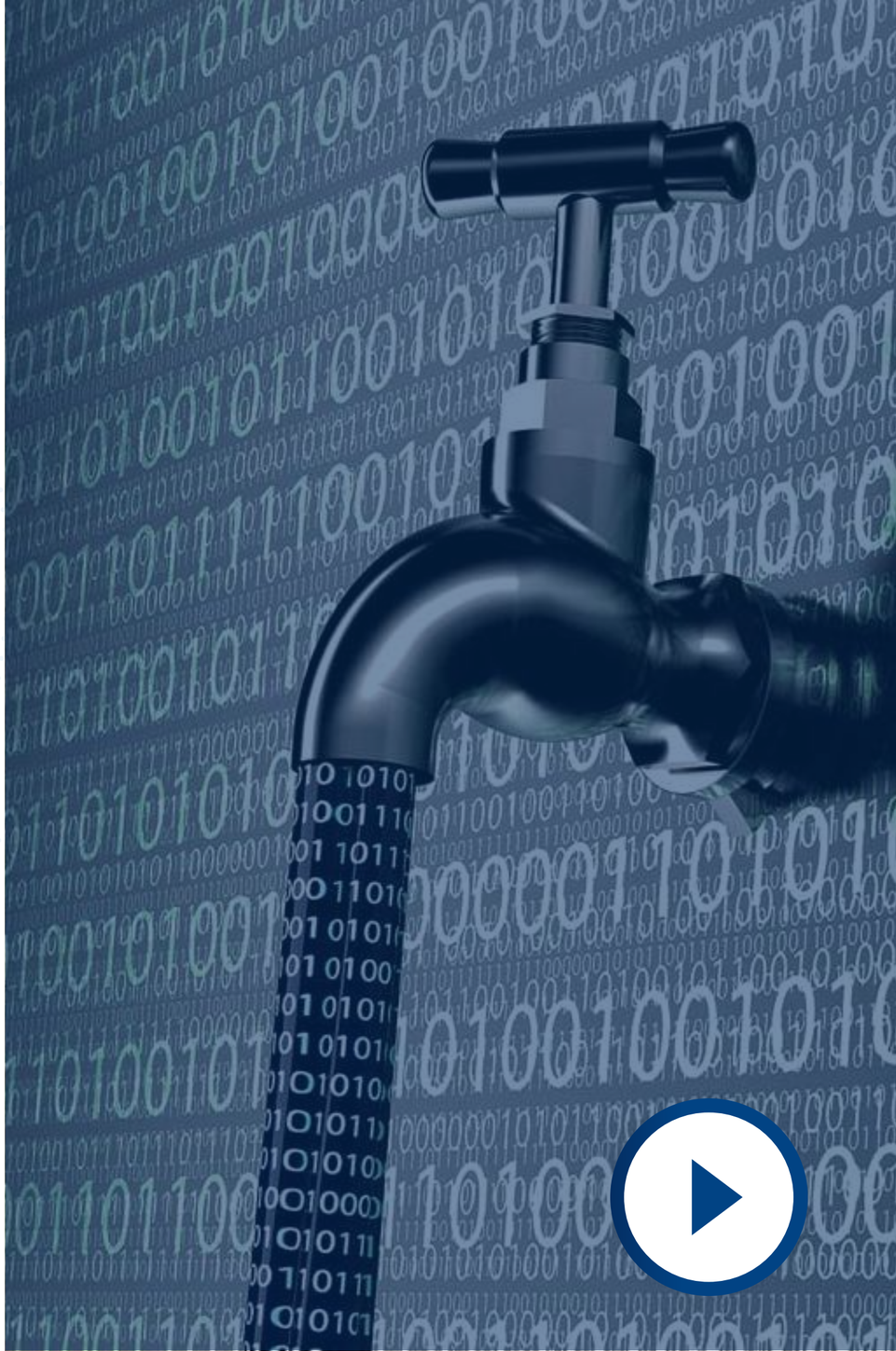
Находим зацепки на ПК Беднякова Валерия

Проводим полный анализ ПК сотрудника

7 Этапы расследования

Проводим анализ целевых систем:

Подтверждаем гипотезу, что файлы с ПК Петрова Игоря были похищены Бедняковым Валерием
.



ФИНАЛ 🏁

Источник слива конфиденциальных данных найден

Инцидент расследован

Какие выводы можно сделать?

1

При расследовании инцидента очень важно комплексно подходить к нему, так как важные улики могут оставаться только в остаточных артефактах

2

Важно иметь возможность быстрого получения нужных артефактов или файлов, благодаря анализу всей сети компании

Контакты

Даниэль Клюев

Эксперт в области извлечения и анализа данных из персональных компьютеров