Данные из DLP как доказательство в судебных спорах

kept

Давайте знакомиться

Олег Безик

Руководитель направления eDiscovery и Digital Forensics в Kept

- В консалтинге с 2014 года
- Опыт организации и проведения крупных проектов по раскрытию доказательств в международных арбитражах, FCPA-расследований, корпоративных расследований, расследований инцидентов ИБ
- Единственный в России сертифицированный профессионал в области eDiscovery (ACEDS)
- Два красных диплома МГТУ им. Н.Э. Баумана

Инцидент: утечка конфиденциальных данных компании

Знакомьтесь, это Bad Guy*

- На протяжении 7 лет работал в компании, последние несколько лет в должности руководителя отдела продаж
- 23 марта 2021 года с его корпоративного компьютера им было отправлено электронное письмо с вложенным файлом
- Вложенный файл **Viruchka_po_magazinam_2019.xlsx** содержал конфиденциальную информацию о выручке всех точек продаж компании за 2019 год
- Файл был отправлен с личной почты **very-badguy@yandex.ru**

Об этом директору по безопасности сообщила корпоративная DLP-система (система предотвращения утечек)

*Изображение создано с помощью сервиса https://thispersondoesnotexist.com/

Содержимое лога DLP

Время и дата

Домен компании

Имя корпоративной учетной записи

Адрес почты отправителя

Описание отправленного файла

Основная проблема:

Логи DLP не содержат доказательств совершения действий конкретным человеком

Судебное разбирательство

[redacted] обратился в суд с исковым заявлением к [redacted], в котором после уточнения исковых требований просил восстановить его на работе в [redacted] в должности Начальника отдела Отдела организации продаж 2 Департамента продаж, взыскать с ответчика средний заработок за время вынужденного прогула – [redacted] руб. [redacted] коп., и компенсацию морального вреда - [redacted] руб.

Восстановить с 22 мая [redacted] года на работе в [redacted] в должности Начальника отдела Отдела организации продаж 2 Департамента продаж.

Взыскать с [redacted] в пользу [redacted] средний заработок за время вынужденного прогула – [redacted] коп., и компенсацию морального вреда – [redacted] руб., а всего – [redacted] коп.

Почему это произошло

- В компании отсутствовало положение о коммерческой тайне
- У компании не было опыта проведения подобных расследований
- Не были собраны объективные и всесторонние доказательства причастности конкретного сотрудника – только логи из DLP
- Компания не наняла независимую профессиональную команду для сбора и анализа доказательств утечки данных

Компания наняла компьютерных криминалистов для проведения независимого расследования

Цель и задачи расследования

kept

ЦЕЛЬ КОМПАНИИ:

Провести независимое расследование и собрать доказательства распространения Bad Guy конфиденциальной информации компании

ЗАДАЧИ КОМПЬЮТЕРНЫХ КРИМИНАЛИСТОВ:

- Идентифицировать потенциальные источники доказательств
- Собрать цифровые данные из идентифицированных источников
- Обнаружить и зафиксировать доказательства использования Bad Guy корпоративного компьютера для отправки файла с конфиденциальными данными
- Подготовить отчет на русском языке для возможного предоставления в судебные органы

Источники цифровых доказательств

kept

Базы данных корпоративных систем

Пример:
1С, СКУД, базы ИТ-служб, Active Directory

Где расположены данные:
- Компьютеры сотрудников бухгалтерии
- Корпоративные сервера или виртуальные машины

К кому идти за данными:
1. К главному бухгалтеру и руководителю HR
2. К главе IT-службы
3. К руководителю службы безопасности

Что содержится:
- Сведения о приеме сотрудника на работу, его должность
- Имя и детали корпоративной учетной записи сотрудника
- Список оборудования, выданного компанией
- Даты и время посещении сотрудником офиса

Записи систем видеонаблюдения

Пример:
Тексты и сканы договоров, документация по проектами, коммерческие предложения, таблица с расчётами и т.д.

Где расположены данные:
- Удаленный сервер компании или здания
- Носитель видеорегистратора

К кому идти за данными:
1. К руководителю службы безопасности

Что содержится:
Видеозаписи, фиксирующие факт нахождения сотрудника на рабочем месте в определенную дату и время

Копия содержимого корпоративного устройства сотрудника

Пример:
Полная побитовая копия содержимого носителей (физического или виртуального)

Где расположены данные:
- Компьютер сотрудника (лэптоп или ПК)
- Виртуальная машина
- Мобильное устройство

К кому идти за данными:
1. К руководителю сотрудника-держателя данных, а после к самому сотруднику
2. К главе IT-службы

Что содержится:
- Хронология использования устройства
- Использование корпоративной учетной записи
- История запуска программ
- История браузера
- История подключения внешних носителей
- И др.

Построение Timeline

- **Timeline** – хронология событий, произошедших на компьютере за определенный период времени
- Минимальный набор данных: дата и время события, **его описание** и источник информации
- Наиболее часто встречающаяся форма – **таблица**
- Программное обеспечение для построения super-timeline: plaso, Autopsy, Axiom Magnet, EnCase, и др.

Дата	Время	Событие	Источник данных	Имя файла
21.03.2021	11:10:40	Логирование учетной записи DESKTOP-D6RP3SB\Very Bad Gu	Журнал Windows	Security.evtx
21.03.2021	11:12:56	Открытие файла C:\Users\Very Bad Guy\Desktop\Docs\Viruch	Файл JumpList	b8ab77100df80ab2.automati
21.03.2021	11:14:09	Запуск программы Microsoft Excel 2016	Файл Prefetch	EXCEL.EXE-9231AABD.pf
21.03.2021	11:15:25	Запуск браузера Mozilla Firefox	Файл Prefetch	FIREFOX.EXE-25FC0A66.pf
21.03.2021	11:16:14	Авторизация в Яндекс.Почту Bad Guy	История браузера Mozilla Firefox	places.sqlite
21.03.2021	11:17:33	Письмо «(Без темы)» — Bad Guy — Яндекс.Почта	История браузера Mozilla Firefox	places.sqlite
21.03.2021	11:17:55	Открытие файла через диалоговое окно Открыть-Сохранить	Файл реестра: OpenSavePidlMRU	NTUSER.dat
21.03.2021	11:17:55	Обращение программы firefox.exe к каталогу My Computer\D	Файл реестра: OpenSavePidlMRU	NTUSER.dat
21.03.2021	11:18:59	Подключение флешки ADATA USB Flash Drive USB Device (S/N	Файл реестра: USBSTOR, MountedDevices	SYSTEM
21.03.2021	11:23:28	Открытие файла E:\Viruchka_po_magazinam_2019.xlsx	Файл JumpList	b8ab77100df80ab2.automati
21.03.2021	11:24:07	Запуск программы Microsoft Excel 2016	Файл Prefetch	EXCEL.EXE-9231AABD.pf
21.03.2021	11:24:07	Открытие файла Viruchka_po_magazinam_2019.xlsx	Файл реестра: R	
21.03.2021	11:24:07	Открытие каталога ADATA UFD (E:)		

Как защитить потенциально релевантные данные

kept

- Все потенциально релевантные данные необходимо защитить от непреднамеренных или преднамеренных удалений, изменений или перемещений

Непреднамеренное воздействие

Программное обеспечение компьютера «затерло» старые записи в системном журнале

Преднамеренное воздействие

Сотрудник очистил историю браузер на своем компьютере после того, как отправил во вне конфиденциальных файл

- Для защиты данных необходимо письменно оповестить сотрудников о том, чтобы они не удаляли и не изменяли потенциально релевантные данные с помощью официального уведомления

Практические советы:

- Укажите предмет спора или расследования
- Приведите примеры места, где релевантные данные могут храниться
- Адресуйте уведомление только тем сотрудникам, кто может обладать релевантными данными или влиять на их целостность
- Предоставьте четкие инструкции по тому, как защитить данные от уничтожения или изменения
- Укажите контакты лиц, с которым можно обсудить возможные проблемы или вопросы

Выводы

- Для работы с цифровыми доказательствами нужна специальная экспертиза
- Логи DLP не являются самодостаточным доказательством причастности конкретного сотрудника к событию ИБ
- Необходимо собирать доказательства из дополнительных источников: базы данных, компьютеры сотрудников, система видеонаблюдения, СКУД и др.
- Все цифровые доказательства должны быть защищены от уничтожения и собраны криминалистически правильно (forensically sound)

Контакты

Илья Шаленков

Партнер,
Руководитель Группы
по оказанию услуг в области
кибербезопасности

T: +7 (903) 792-80-77
E: IShalenkov@kept.ru

Олег Безик

Заместитель директора,
Группа по оказанию услуг в
области кибербезопасности
Kept

T: +7 (926) 497-46-32
E: obezik@kept.ru

www.kept.ru