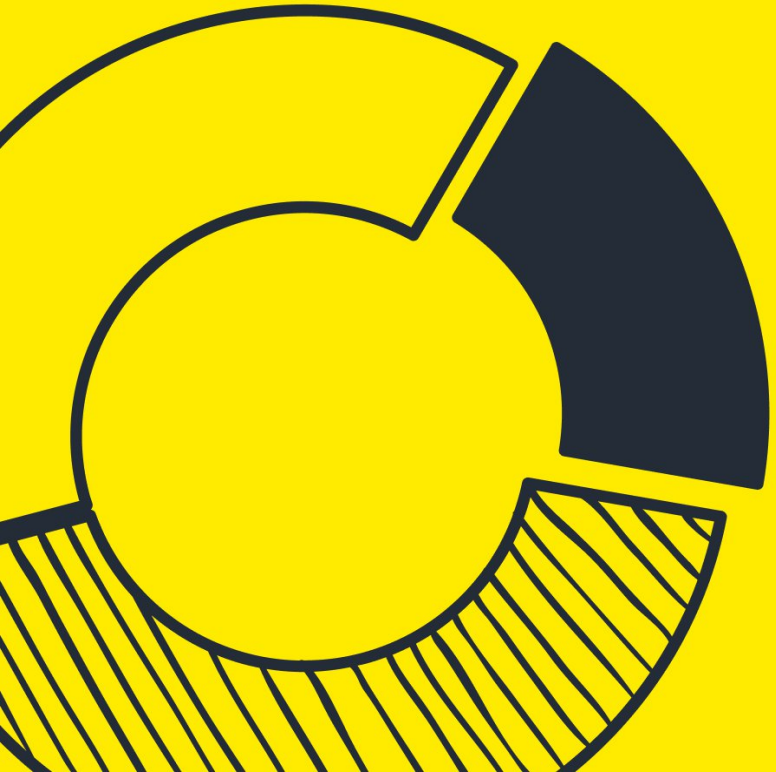
НИКИТА ВЬЮГИН

МЕНЕДЖЕР ПРОЕКТОВ

MKO SYSTEMS

РАССЛЕДОВАНИЕ КИБЕРИНЦИДЕНТОВ НА ПРАКТИКЕ

СТАТИСТИКА



1-3 КВАРТАЛ 2023 Г.:

73% АТАК

являлись целевыми

ЦЕЛИ:

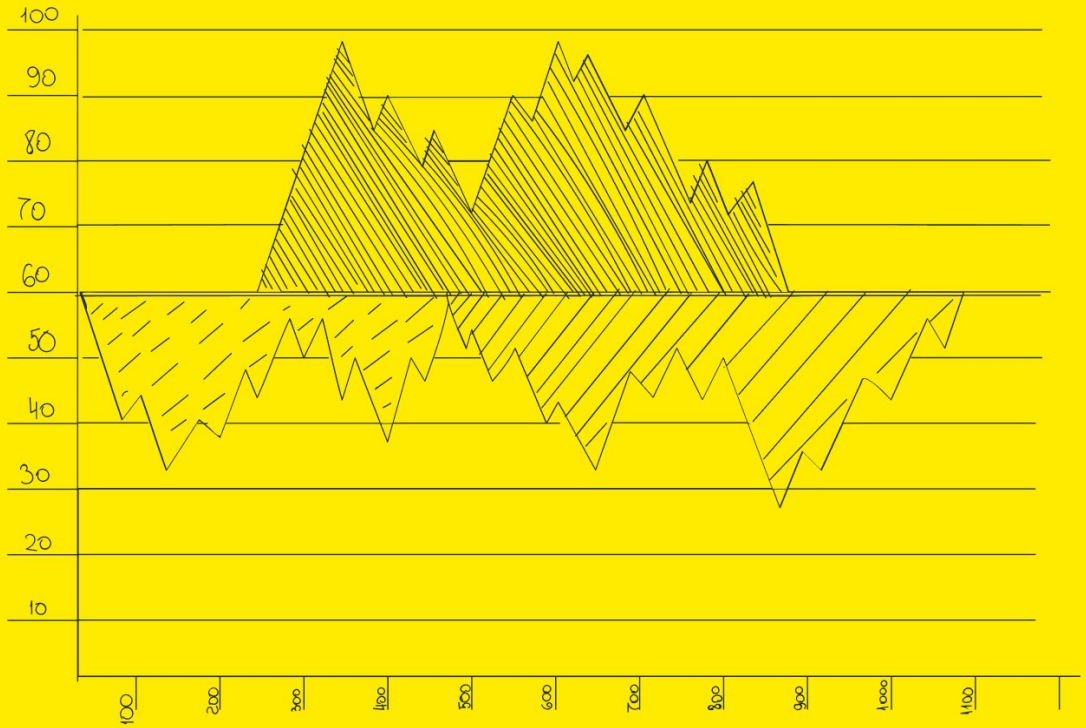
58%

конфиденциальная информация

41%

нарушение деятельности компании

СТАТИСТИКА



43%

персональные данные

16%

учетные данные

13%

коммерческая тайна

СТАТИСТИКА

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ВСТРЕЧАЕТСЯ В КАЖДОЙ 2-Й АТАКЕ:

81%

фишинг через электронную почту (для организаций)

53% АТАК

фродсайты (частные лица)

СТАТИСТИКА

1-Й КВАРТАЛ 2024 ГОДА

Доля кибератак высокой критичности выросла

в 3 раза

до 80%

увеличилась доля таких инцидентов с применением ВПО

в 4 раза

увеличилась доля веб-атак (до 15%)

ВАРИАНТЫ

РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

- Быстрое восстановление работы компании
- Сбор улик и доказательств для расследования

ЦЕЛИ

РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

- Деньги-деньги-деньги!
- 152 ФЗ
- Штрафы для финансовых организаций
- Повышение уровня кибербезопасности
- Разработка регламентов для реагирования

ЧТО ТАКОЕ

DFIR

Digital Forensics and Incident Response

«ЦИФРОВАЯ КРИМИНАЛИСТИКА И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ» – специализированная область, охватывающая выявление, устранение и расследование инцидентов кибербезопасности в том числе с применением криминалистических практик.

4 ОСНОВНЫХ ЭТАПА

ПЕРВИЧНОЙ РАБОТЫ С ЦИФРОВЫМИ ДОКАЗАТЕЛЬСТВАМИ

- Идентификация
- Сбор
- Извлечение
- Хранение

ISO/IEC 27037:2012

ИДЕНТИФИКАЦИЯ

- Кто вовлечен в инцидент?
- Что случилось?
- Когда произошел инцидент?
- Где произошел инцидент?
- Как произошел инцидент?

СБОР

Изолирование «места преступления», идентификация и документация устройств и источников данных:

- Техническое состояние (включено/выключено/режим ожидания)
- Физическое состояние (царапины, следы вскрытия и т.д.)
- Серийные номера
- Модели
- Сетевые соединения
- Другое

ИЗВЛЕЧЕНИЕ ДАННЫХ

Если нет витальных предпосылок к обратному, этот этап должен проводиться не «на месте», а в специально оборудованной лаборатории.

ХРАНЕНИЕ ДАННЫХ

- Предотвращение модификации данных
- Обеспечение их целостности

АНАЛИЗ

(ИЗУЧЕНИЕ И ИНТЕРПРЕТАЦИЯ ДАННЫХ)

- Все данные, аспекты и доступная информация переданы эксперту
- Поставлены и разъяснены все цели и задачи расследования
- Воссоздание хронологии событий инцидента

ОТЧЕТ

- Описывает все действия на каждом этапе расследования
- Описывает все результаты каждого из этапов
- Понятен и прозрачен
- На базе отчета будет написан регламент (обновлен Playbook)

ПРАКТИЧЕСКИЙ

КЕЙС

- Дистрибутив программы в открытом доступе в ТГ
- Лицензия на 1 год, от 25 октября
- Все лицензии проходят через службу поддержки и ее руководителя

ЗАДАЧА

- Установить, причастна ли служба поддержки к сливу
- Собрать прямые или косвенные доказательства
- Начать с PC руководителя службы безопасности

РИСУНОК 1

ЛЕНТА СОБЫТИЙ В MK ENTERPRISE С КРИТЕРИЯМИ ПОИСКА ПО ДАТЕ

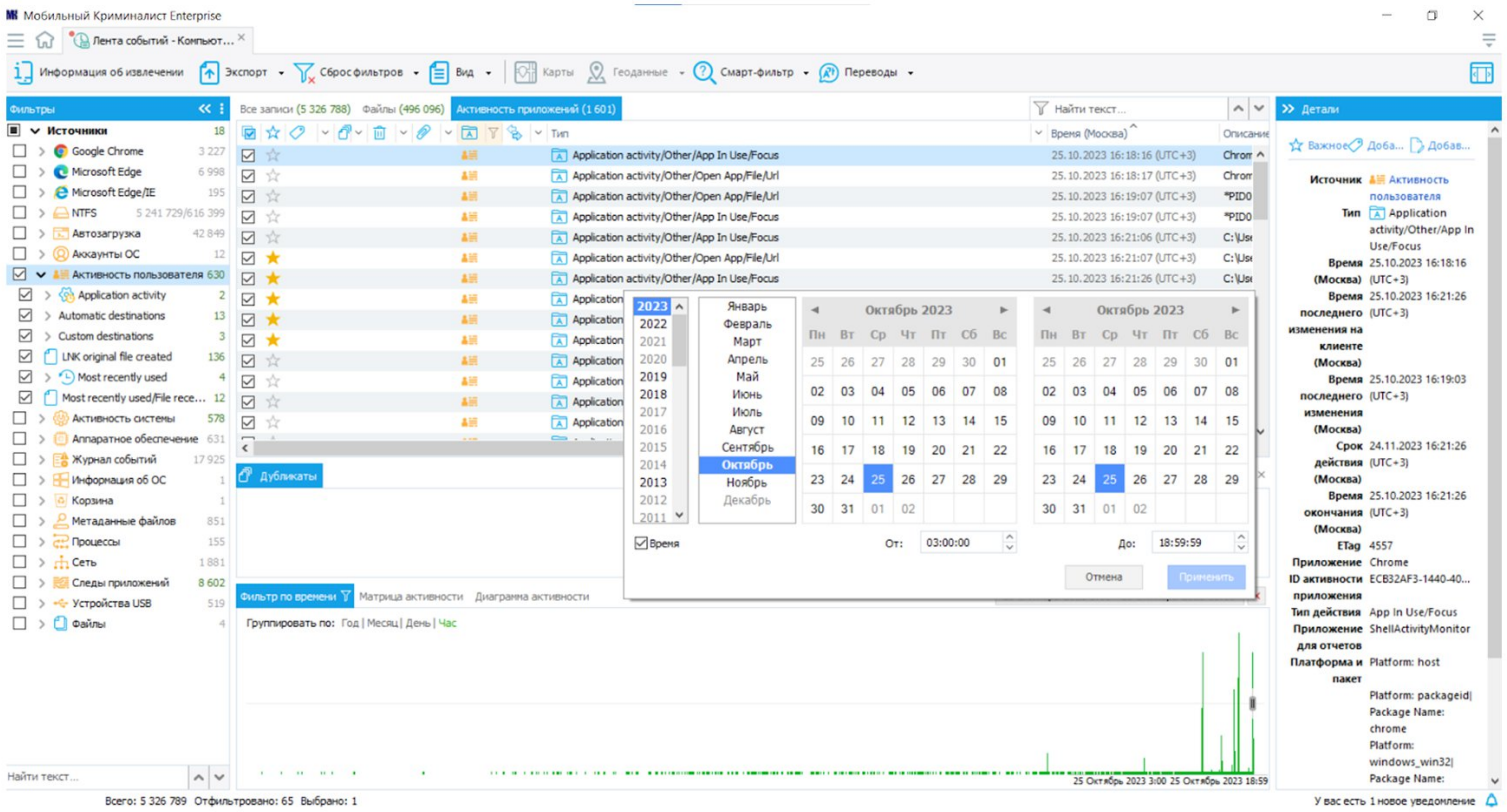


РИСУНОК 2

АНАЛИЗ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ В МК ENTERPRISE ПО ДАТЕ И ВРЕМЕНИ

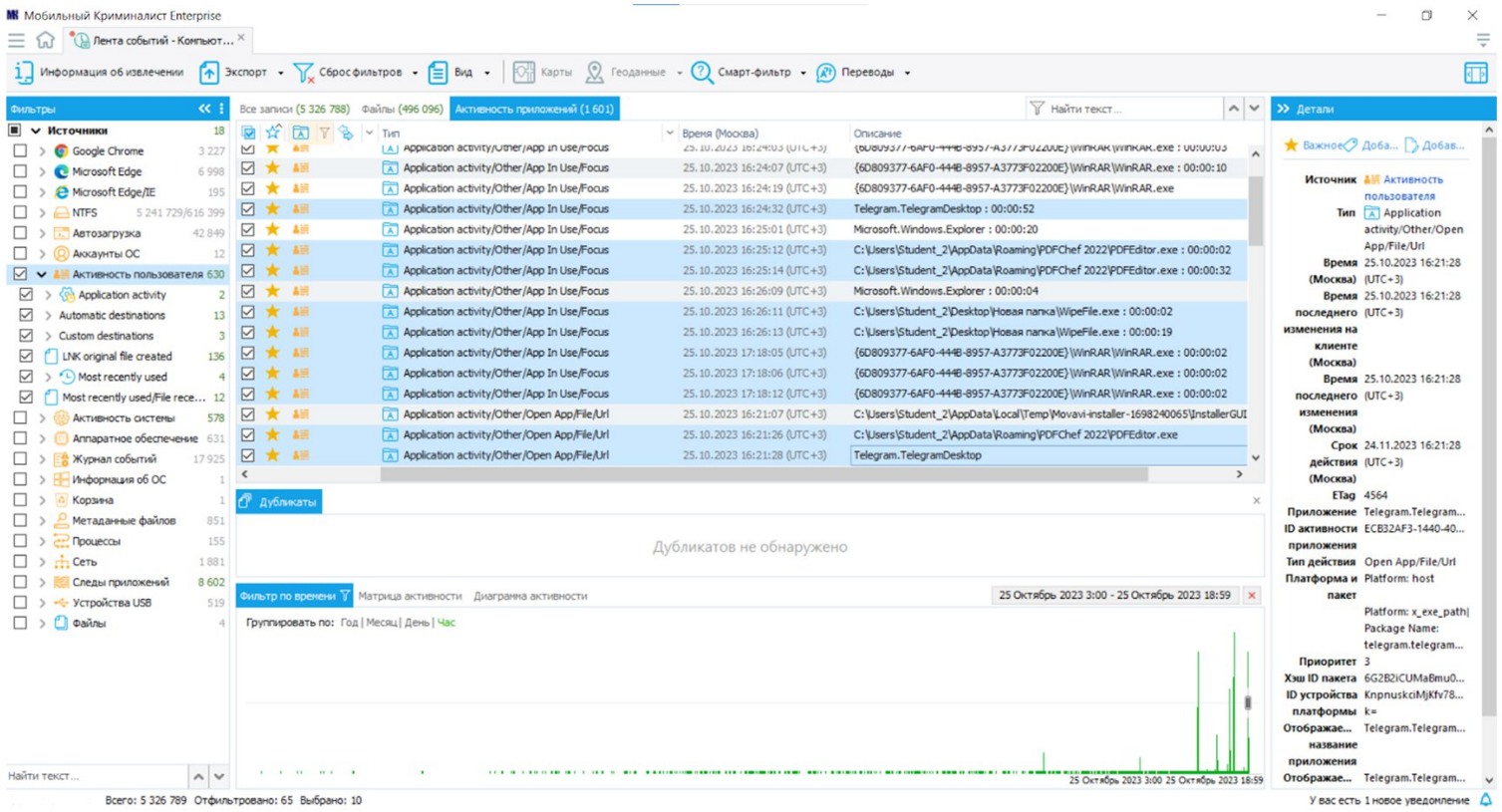


РИСУНОК 3

ВЫБОР ПУНКТА «АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЯ» В ГЛАВНОМ МЕНЮ МК ENTERPRISE

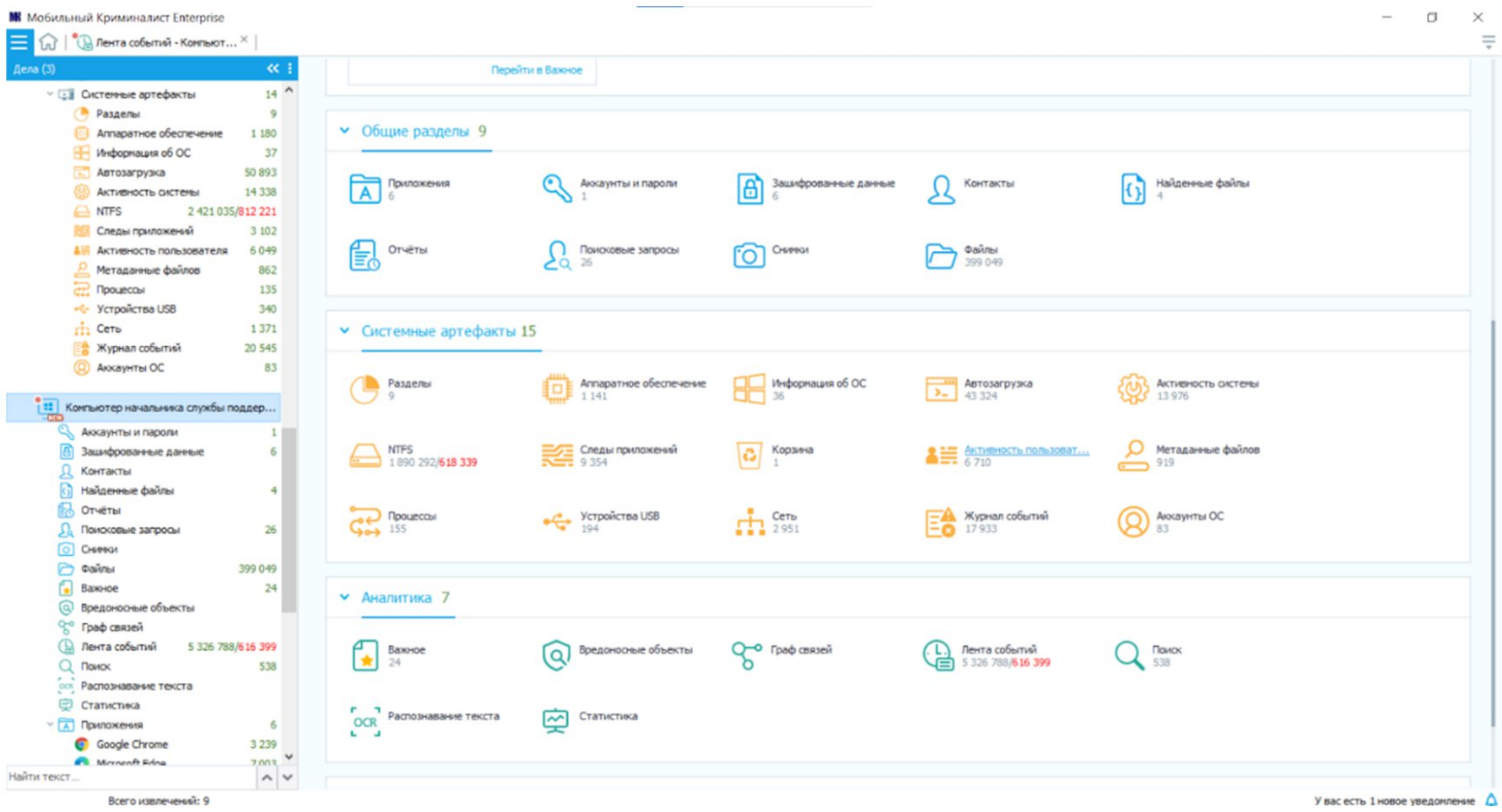


РИСУНОК 4

АНАЛИЗ ПАПОК И ФАЙЛОВ В МК ENTERPRISE

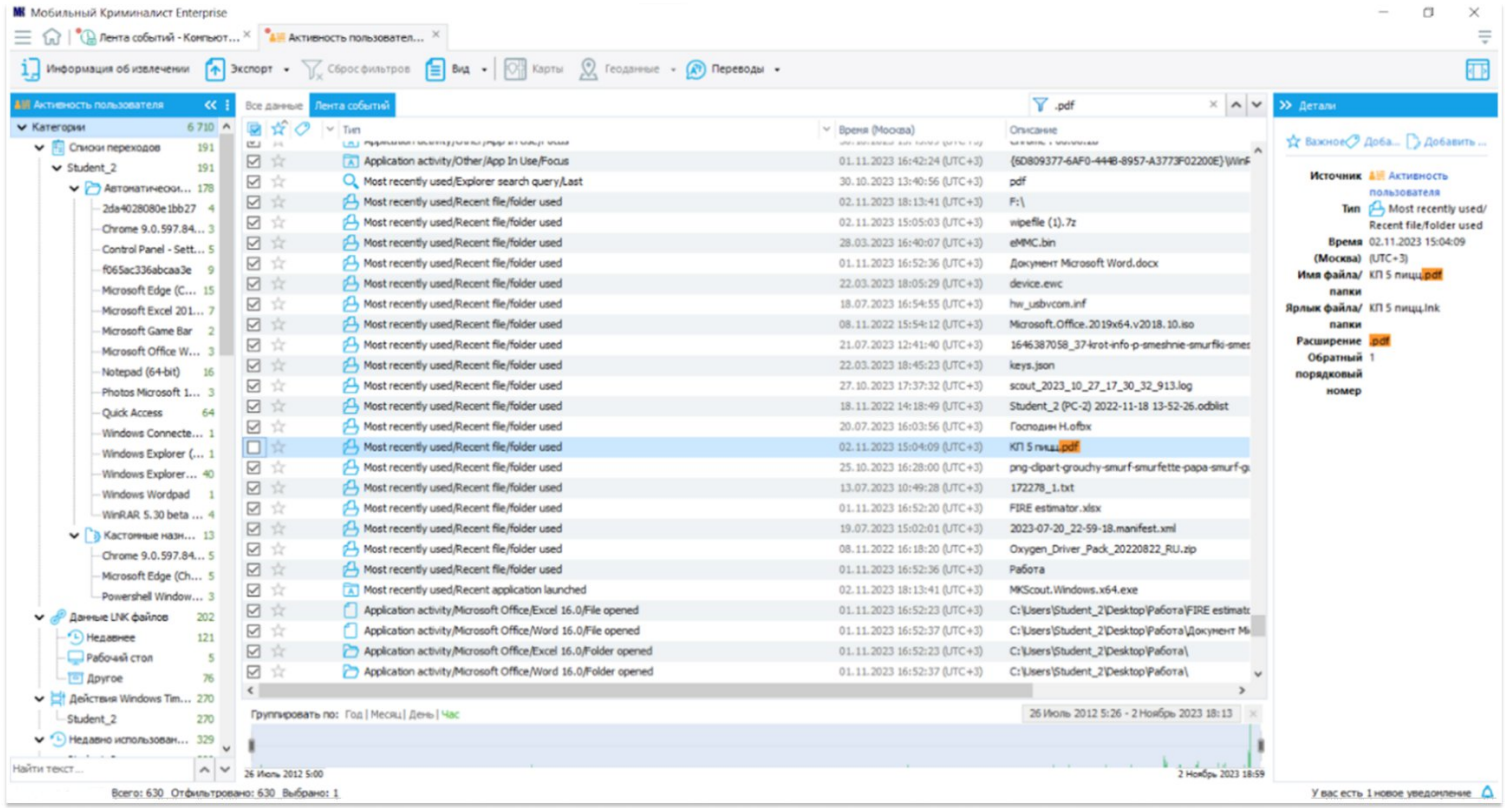
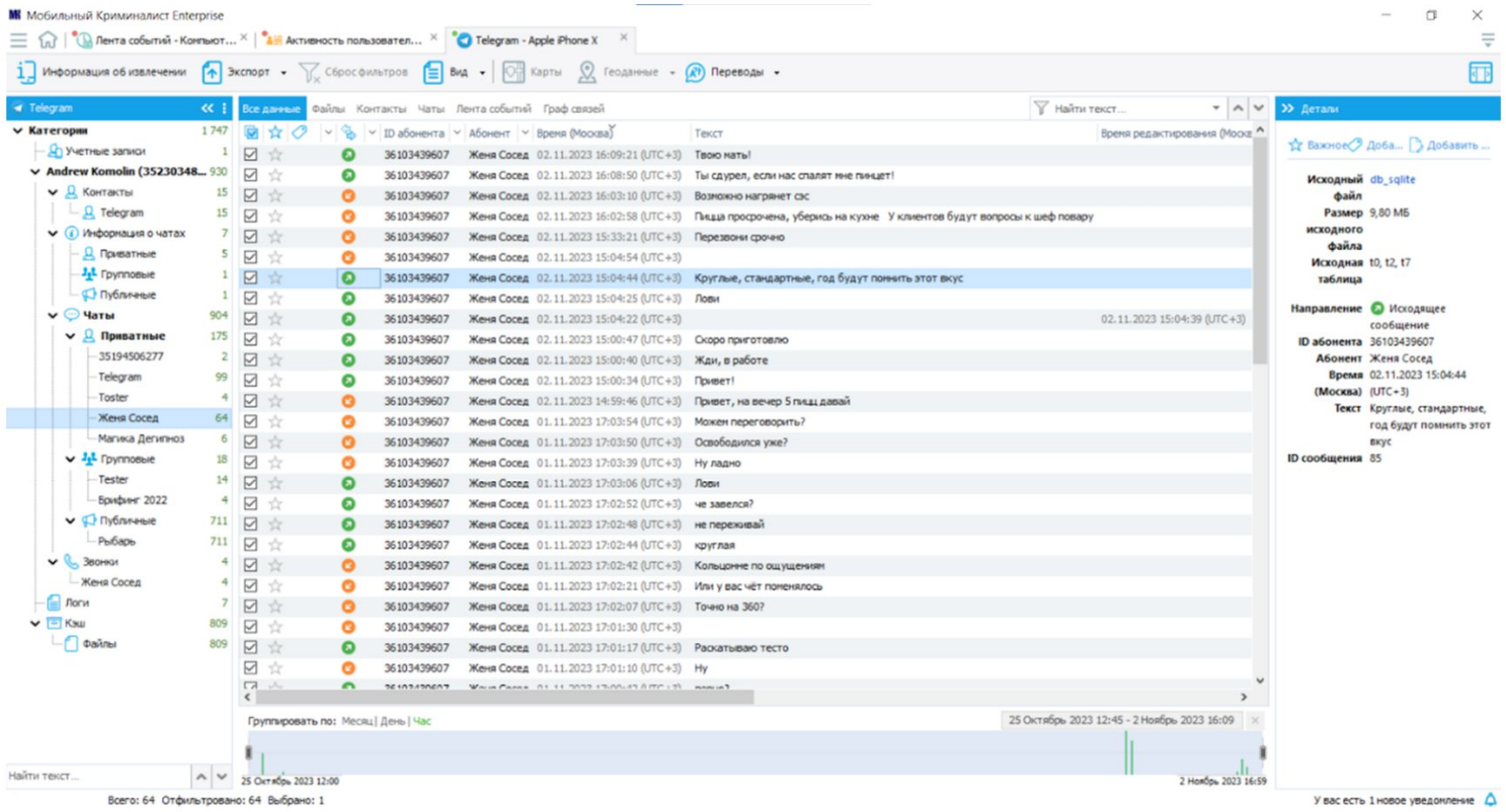


РИСУНОК 5

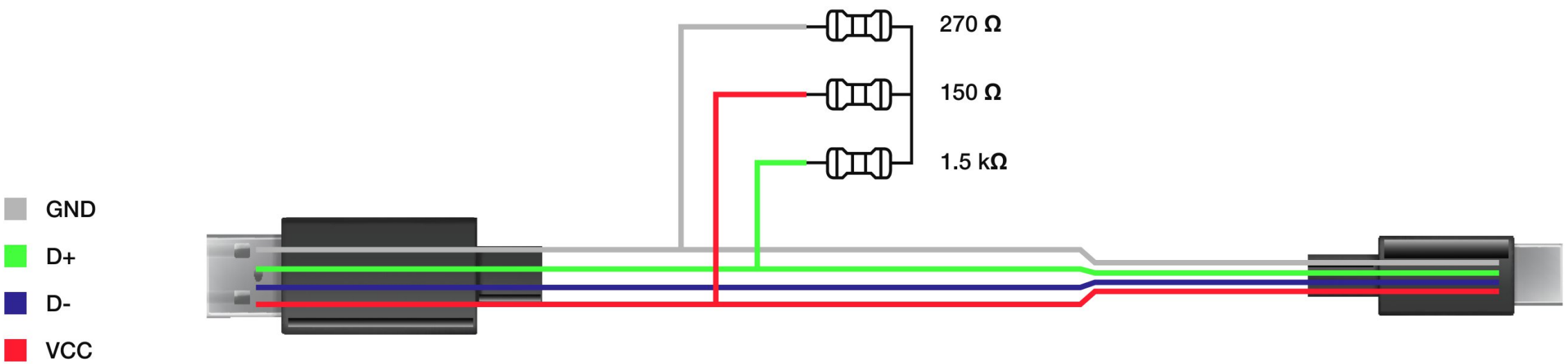
АНАЛИЗ TELEGRAM ПОЛЬЗОВАТЕЛЯ В MK ENTERPRISE



ИТОГ

- Руководитель службы безопасности в сговоре с партнером продавал ПО по «серой» схеме, используя «особенный» язык
- На базе расследования создан отчет и передан в службу безопасности компании
- На базе инцидента департаментами ИБ, ИТ и СБ были созданы новые регламенты для предотвращения подобного рода инцидентов в будущем

#СОБЕРИСАМ



РАЗБЕРИСАМ

СПАСИБО

КОНТАКТЫ:

+7 (495) 909-92-78

clients@mko-systems.ru

mko-systems.ru