

# НИКИТА ВЬЮГИН

МЕНЕДЖЕР ПРОЕКТОВ

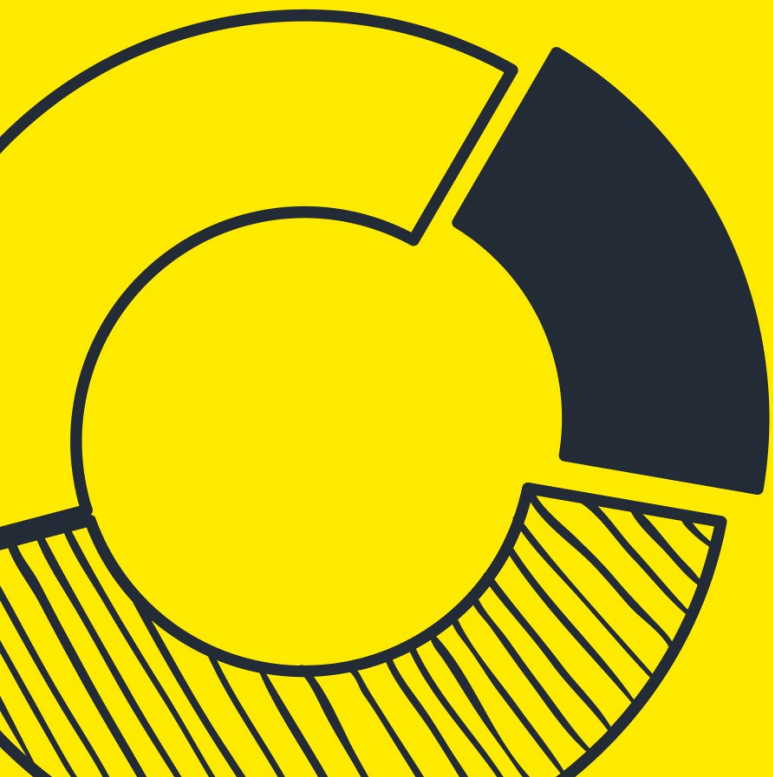


**MIKO**  
SYSTEMS

# РАССЛЕДОВАНИЕ КИБЕРИНЦИДЕНТОВ НА ПРАКТИКЕ



# СТАТИСТИКА



1-3 КВАРТАЛ 2023 Г.:

**73% АТАК**

являлись целевыми

**ЦЕЛИ:**

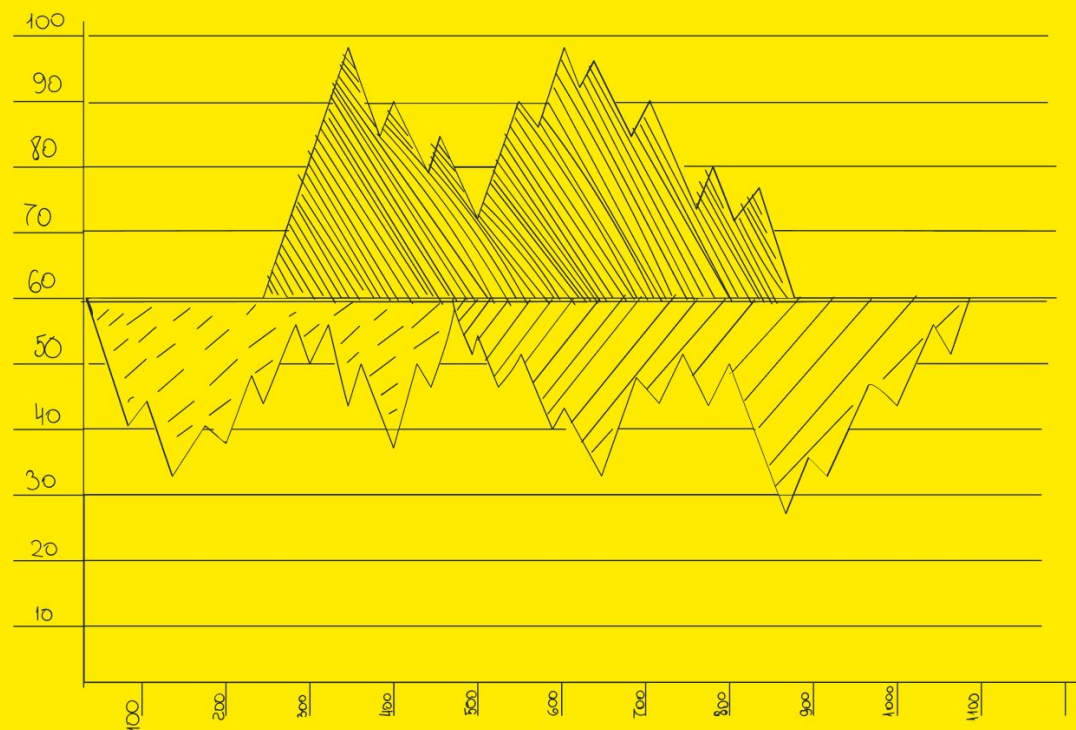
**58%**

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**

**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 ДАНЫХ)

- 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 РС руководителя службы безопасности

# РИСУНОК 1

## ЛЕНТА СОБЫТИЙ В МК ENTERPRISE С КРИТЕРИЯМИ ПОИСКА ПО ДАТЕ

The screenshot displays the 'Мобильный Криминалист Enterprise' (Mobile Criminalist Enterprise) software interface. The main window shows a list of events under the 'Активность приложений' (Application Activity) filter. The interface includes a sidebar with various filters, a central table of events, and a calendar view for filtering by date. A detailed view of a selected event is shown on the right side.

**Список источников (Filters):**

- Google Chrome: 3 227
- Microsoft Edge: 6 998
- Microsoft Edge/IE: 195
- NTFS: 5 241 729/6 16 399
- Автозагрузка: 42 849
- Аккаунты ОС: 12
- Активность пользователя: 630
- Application activity: 2
- Automatic destinations: 13
- Custom destinations: 3
- LNK original file created: 136
- Most recently used: 4
- Most recently used/File rec...: 12
- Активность системы: 578
- Аппаратное обеспечение: 631
- Журнал событий: 17 925
- Информация об ОС: 1
- Корзина: 1
- Метаданные файлов: 851
- Процессы: 155
- Сеть: 1 881
- Следы приложений: 8 602
- Устройства USB: 519
- Файлы: 4

**Таблица событий (Table):**

Источники	Тип	Время (Москва)	Описание
Application activity	Application activity/Other/App In Use/Focus	25.10.2023 16:18:16 (UTC+3)	Chrome
Application activity	Application activity/Other/Open App/File/Url	25.10.2023 16:18:17 (UTC+3)	Chrome
Application activity	Application activity/Other/Open App/File/Url	25.10.2023 16:19:07 (UTC+3)	*PIDO
Application activity	Application activity/Other/App In Use/Focus	25.10.2023 16:19:07 (UTC+3)	*PIDO
Application activity	Application activity/Other/App In Use/Focus	25.10.2023 16:21:06 (UTC+3)	C:\Use
Application activity	Application activity/Other/Open App/File/Url	25.10.2023 16:21:07 (UTC+3)	C:\Use
Application activity	Application activity/Other/App In Use/Focus	25.10.2023 16:21:26 (UTC+3)	C:\Use

**Календарь (Calendar):**

Октябрь 2023

Пн	Вт	Ср	Чт	Пт	Сб	Вс
25	26	27	28	29	30	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	01	02			

**Детали события (Event Details):**

- Источник: Активность пользователя
- Тип: Application activity/Other/App In Use/Focus
- Время (Москва): 25.10.2023 16:18:16 (UTC+3)
- Время последнего изменения на клиенте: 25.10.2023 16:19:03 (UTC+3)
- Время последнего изменения (Москва): 24.11.2023 16:21:26 (UTC+3)
- Срок действия (Москва): 25.10.2023 16:21:26 (UTC+3)
- Время окончания (Москва): 25.10.2023 16:21:26 (UTC+3)
- Этап: 4557
- Приложение: Chrome
- ID активности: EC832AF3-1440-40...
- Тип действия: App In Use/Focus
- Приложение для отчетов: ShellActivityMonitor
- Платформа и пакет: Platform: host
- Platform: packageid]
- Package Name: chrome
- Platform: windows\_win32]
- Package Name: windows\_win32]

У вас есть 1 новое уведомление

# РИСУНОК 2

## АНАЛИЗ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ В МК ENTERPRISE ПО ДАТЕ И ВРЕМЕНИ

Мобильный Криминалист Enterprise

Информация об извлечении | Экспорт | Сброс фильтров | Вид | Карты | Геоданные | Smart-фильтр | Переводы

Фильтры: Все записи (5 326 788) | Файлы (496 096) | Активность приложений (1 601)

Источники	Тип	Время (Москва)	Описание
Google Chrome	Application activity/Other/App In Use/Focus	25.10.2023 16:24:07 (UTC+3)	{60809377-6AF0-444B-8957-A3773F02200E} WinRAR (WinRAR.exe : 00:00:10)
Microsoft Edge	Application activity/Other/App In Use/Focus	25.10.2023 16:24:19 (UTC+3)	{60809377-6AF0-444B-8957-A3773F02200E} WinRAR (WinRAR.exe
Microsoft Edge/IE	Application activity/Other/App In Use/Focus	25.10.2023 16:24:32 (UTC+3)	Telegram.TelegramDesktop : 00:00:52
NTFS	Application activity/Other/App In Use/Focus	25.10.2023 16:25:01 (UTC+3)	Microsoft.Windows.Explorer : 00:00:20
Автозагрузка	Application activity/Other/App In Use/Focus	25.10.2023 16:25:12 (UTC+3)	C:\Users\Student_2\AppData\Roaming\PDFChef 2022\PDFEditor.exe : 00:00:02
Аккаунты ОС	Application activity/Other/App In Use/Focus	25.10.2023 16:25:14 (UTC+3)	C:\Users\Student_2\AppData\Roaming\PDFChef 2022\PDFEditor.exe : 00:00:32
Активность пользователя	Application activity/Other/App In Use/Focus	25.10.2023 16:25:09 (UTC+3)	Microsoft.Windows.Explorer : 00:00:04
Application activity	Application activity/Other/App In Use/Focus	25.10.2023 16:26:11 (UTC+3)	C:\Users\Student_2\Desktop\Новая папка\WipeFile.exe : 00:00:02
Automatic destinations	Application activity/Other/App In Use/Focus	25.10.2023 16:26:13 (UTC+3)	C:\Users\Student_2\Desktop\Новая папка\WipeFile.exe : 00:00:19
Custom destinations	Application activity/Other/App In Use/Focus	25.10.2023 17:18:05 (UTC+3)	{60809377-6AF0-444B-8957-A3773F02200E} WinRAR (WinRAR.exe : 00:00:02
LNK original file created	Application activity/Other/App In Use/Focus	25.10.2023 17:18:06 (UTC+3)	{60809377-6AF0-444B-8957-A3773F02200E} WinRAR (WinRAR.exe : 00:00:02
Most recently used	Application activity/Other/App In Use/Focus	25.10.2023 17:18:12 (UTC+3)	{60809377-6AF0-444B-8957-A3773F02200E} WinRAR (WinRAR.exe : 00:00:02
Most recently used/File reces...	Application activity/Other/Open App/File/Url	25.10.2023 16:21:07 (UTC+3)	C:\Users\Student_2\AppData\Local\Temp\Movavi-installer-169824065\InstallerGUI
Активность системы	Application activity/Other/Open App/File/Url	25.10.2023 16:21:26 (UTC+3)	C:\Users\Student_2\AppData\Roaming\PDFChef 2022\PDFEditor.exe
Аппаратное обеспечение	Application activity/Other/Open App/File/Url	25.10.2023 16:21:28 (UTC+3)	Telegram.TelegramDesktop

Дубликаты

Дубликаты не обнаружено

Фильтр по времени | Матрица активности | Диаграмма активности

Группировать по: Год | Месяц | День | Час

Всего: 5 326 789 | Отфильтровано: 65 | Выбрано: 10

25 Октября 2023 3:00 - 25 Октября 2023 18:59

У вас есть 1 новое уведомление

Источники: Активность пользователя

Тип: Application activity/Other/Open App/File/Url

Время (Москва): 25.10.2023 16:21:28 (UTC+3)

Время последнего изменения на клиенте (Москва): 25.10.2023 16:21:28 (UTC+3)

Время последнего изменения (Москва): 25.10.2023 16:21:28 (UTC+3)

Срок действия (Москва): 24.11.2023 16:21:28 (UTC+3)

Этап: 4564

Приложение: Telegram.Telegram...

ID активности приложения: EC832AF3-1440-40...

Тип действия: Open App/File/Url

Платформа и пакет: Platform: host

Platform: x\_exe\_path | Package Name: telegram.telegram...

Приоритет: 3

Хэш ID пакета: 6G2B2iCUMaVmu0...

ID устройства: kprnuskoiMkfv78...

платформы: k=

Отображае...: Telegram.Telegram...

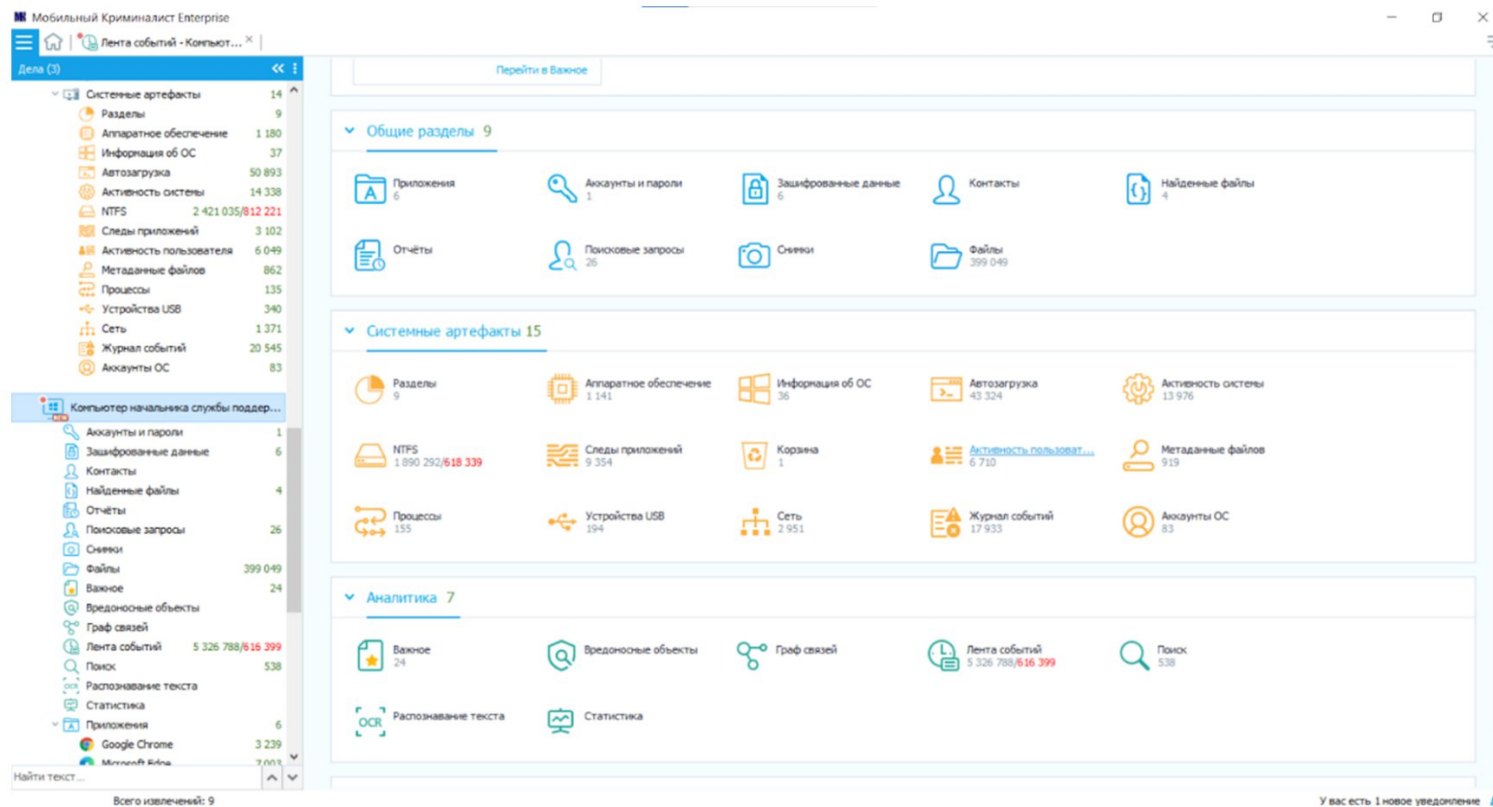
название приложения

Отображае...: Telegram.Telegram...



# РИСУНОК 3

ВЫБОР ПУНКТА  
«АКТИВНОСТЬ  
ПОЛЬЗОВАТЕЛЯ»  
В ГЛАВНОМ МЕНЮ МК  
ENTERPRISE



# РИСУНОК 4

## АНАЛИЗ ПАПОК И ФАЙЛОВ В МК ENTERPRISE

The screenshot displays the 'Мобильный Криминалист Enterprise' software interface. The main window shows a list of user activities under the 'Активность пользователя' tab. The table includes columns for 'Тип' (Type), 'Время (Москва)' (Time (Moscow)), and 'Описание' (Description). A sidebar on the left shows a category tree, and a details panel on the right shows file properties for a selected PDF document.

Тип	Время (Москва)	Описание
Application activity/Other/App In Use/Focus	01.11.2023 16:42:24 (UTC+3)	(6D809377-6AF0-444B-8957-A3773F02200E)\WinF
Most recently used/Explorer search query/Last	30.10.2023 13:40:56 (UTC+3)	pdf
Most recently used/Recent file/folder used	02.11.2023 18:13:41 (UTC+3)	F:\
Most recently used/Recent file/folder used	02.11.2023 15:05:03 (UTC+3)	wipefile (1).7z
Most recently used/Recent file/folder used	28.03.2023 16:40:07 (UTC+3)	eMMC.bn
Most recently used/Recent file/folder used	01.11.2023 16:52:36 (UTC+3)	Документ Microsoft Word.docx
Most recently used/Recent file/folder used	22.03.2023 18:05:29 (UTC+3)	device.exe
Most recently used/Recent file/folder used	18.07.2023 16:54:55 (UTC+3)	hw_usbvcam.inf
Most recently used/Recent file/folder used	08.11.2022 15:54:12 (UTC+3)	Microsoft.Office.2019x64.v2018.10.iso
Most recently used/Recent file/folder used	21.07.2023 12:41:40 (UTC+3)	1646387058_37-krot-info-p-smeshnie-smurf-flo-smes
Most recently used/Recent file/folder used	22.03.2023 18:45:23 (UTC+3)	keys.json
Most recently used/Recent file/folder used	27.10.2023 17:37:32 (UTC+3)	scout_2023_10_27_17_30_32_913.log
Most recently used/Recent file/folder used	18.11.2022 14:18:49 (UTC+3)	Student_2 (PC-2) 2022-11-18 13-52-26.odtblst
Most recently used/Recent file/folder used	20.07.2023 16:03:56 (UTC+3)	Господин Н.офш
Most recently used/Recent file/folder used	02.11.2023 15:04:09 (UTC+3)	КП 5 пнци.pdf
Most recently used/Recent file/folder used	25.10.2023 16:28:00 (UTC+3)	png-clpart-grouchy-smurf-smurfette-papa-smurf-p
Most recently used/Recent file/folder used	13.07.2023 10:49:28 (UTC+3)	172278_1.txt
Most recently used/Recent file/folder used	01.11.2023 16:52:20 (UTC+3)	FIRE estimator.xlsx
Most recently used/Recent file/folder used	19.07.2023 15:02:01 (UTC+3)	2023-07-20_22-59-18.manifest.xml
Most recently used/Recent file/folder used	08.11.2022 16:18:20 (UTC+3)	Oxygen_Driver_Pack_20220822_RU.zip
Most recently used/Recent file/folder used	01.11.2023 16:52:36 (UTC+3)	Работа
Most recently used/Recent application launched	02.11.2023 18:13:41 (UTC+3)	MKScout.Windows.v64.exe
Application activity/Microsoft Office/Excel 16.0/File opened	01.11.2023 16:52:23 (UTC+3)	C:\Users\Student_2\Desktop\Работа\FIRE estimat
Application activity/Microsoft Office/Word 16.0/File opened	01.11.2023 16:52:37 (UTC+3)	C:\Users\Student_2\Desktop\Работа\Документ М
Application activity/Microsoft Office/Excel 16.0/Folder opened	01.11.2023 16:52:23 (UTC+3)	C:\Users\Student_2\Desktop\Работа\
Application activity/Microsoft Office/Word 16.0/Folder opened	01.11.2023 16:52:37 (UTC+3)	C:\Users\Student_2\Desktop\Работа\

Details panel for 'КП 5 пнци.pdf':

- Источник: Активность пользователя
- Тип: Most recently used/Recent file/folder used
- Время (Москва): 02.11.2023 15:04:09 (UTC+3)
- Имя файла/папки: КП 5 пнци.pdf
- Ярлык файла/папки: КП 5 пнци.link
- Расширение: pdf
- Обратный порядковый номер: 1

# РИСУНОК 5

## АНАЛИЗ TELEGRAM ПОЛЬЗОВАТЕЛЯ В МК ENTERPRISE

Мобильный Криминалист Enterprise

Telegram - Apple iPhone X

Информация об извлечениях | Экспорт | Сброс фильтров | Вид | Карты | Геоданные | Переводы

Telegram

Категория	Всего данных	Файлы	Контакты	Чаты	Лента событий	Граф связей	Найти текст...	Детали
Учетные записи	1747							
Andrew Komolin (35230348...)	930							
Контакты	15							
Telegram	15							
Информация о чатах	7							
Приватные	5							
Групповые	1							
Публичные	1							
Чаты	904							
Приватные	175							
35194506277	2							
Telegram	99							
Tester	4							
Женя Сосед	64							
Малыга Дегизноз	6							
Групповые	18							
Tester	14							
Брифинг 2022	4							
Публичные	711							
Рыбарь	711							
Звонки	4							
Женя Сосед	4							
Логи	7							
Кли	809							
Файлы	809							

Время редактирования (Москва)

Исходный файл db\_sqli  
Размер 9,80 МБ  
Исходная таблица 10, 12, 17  
Направление Исходящее сообщение  
ID абонента 36103439607  
Абонент Женя Сосед  
Время 02.11.2023 15:04:44 (Москва) (UTC+3)  
Текст Круглые, стандартные, год будут помнить этот вкус  
ID сообщения 85

У вас есть 1 новое уведомление

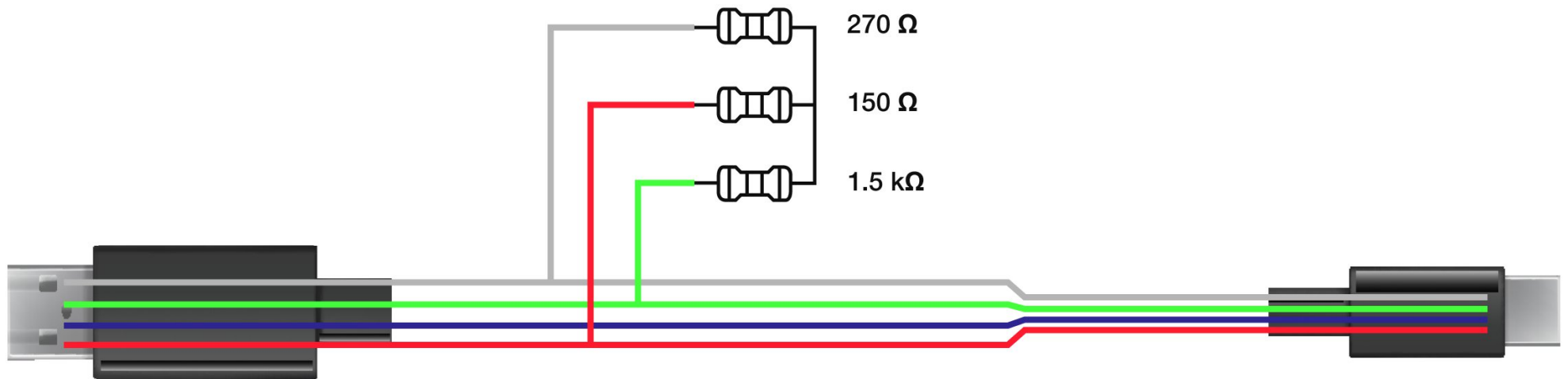
# ИТОГ

- 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

- GND
- D+
- D-
- VCC







# РАЗБЕРИСАМ





# СПАСИБО

## КОНТАКТЫ:

 +7 (495) 909-92-78

 [clients@mko-systems.ru](mailto:clients@mko-systems.ru)

 [mko-systems.ru](http://mko-systems.ru)