BEHOLDER
IS
HERE

исследования
и консалтинг

# ВИДЫ И СПОСОБЫ ПРОВЕДЕНИЯ ХОРОШЕЙ РЫБАЛКИ

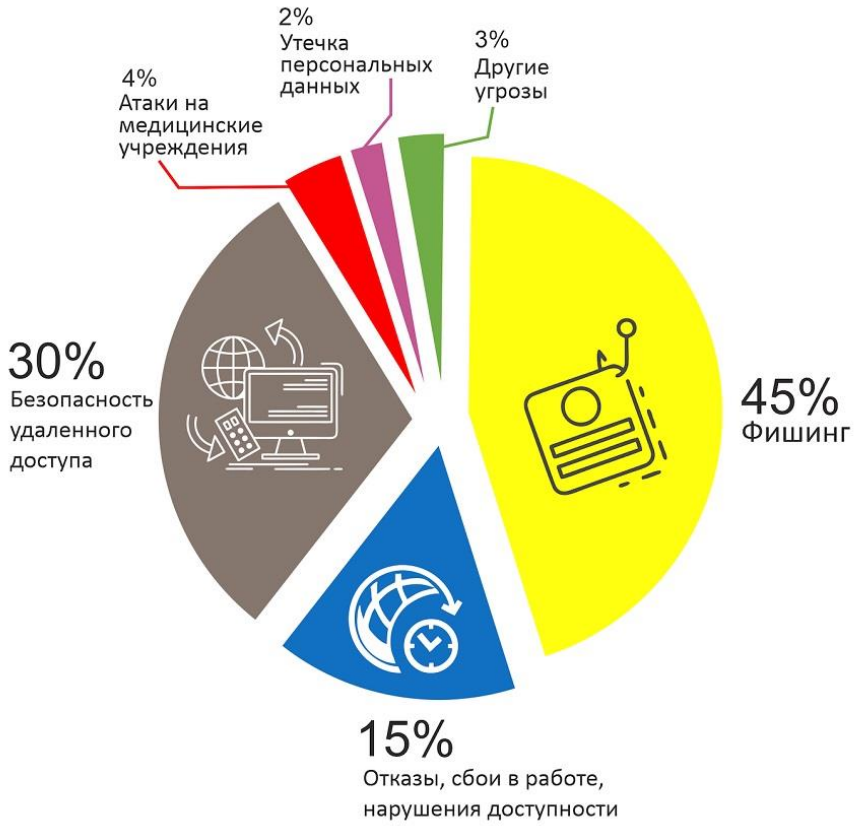

**КОД ИБ: Калининград**

**БОРОЩУК ДМИТРИЙ**

# «КИБЕР БЕЗОПАСНОСТЬ» – ВСЯ СУТЬ:

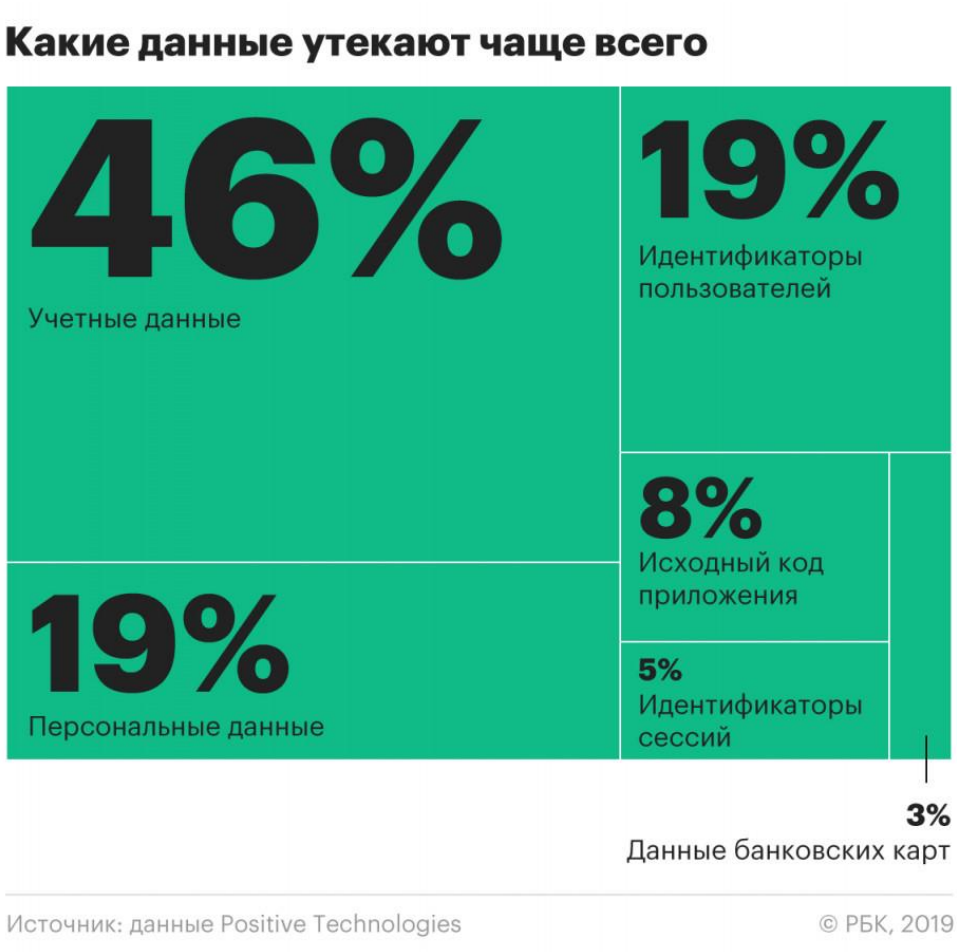
# «КИБЕР БЕЗОПАСНОСТЬ» – ВСЯ СУТЬ:

# НЕМНОГО СВЕЖЕЙ СТАТИСТИКИ.

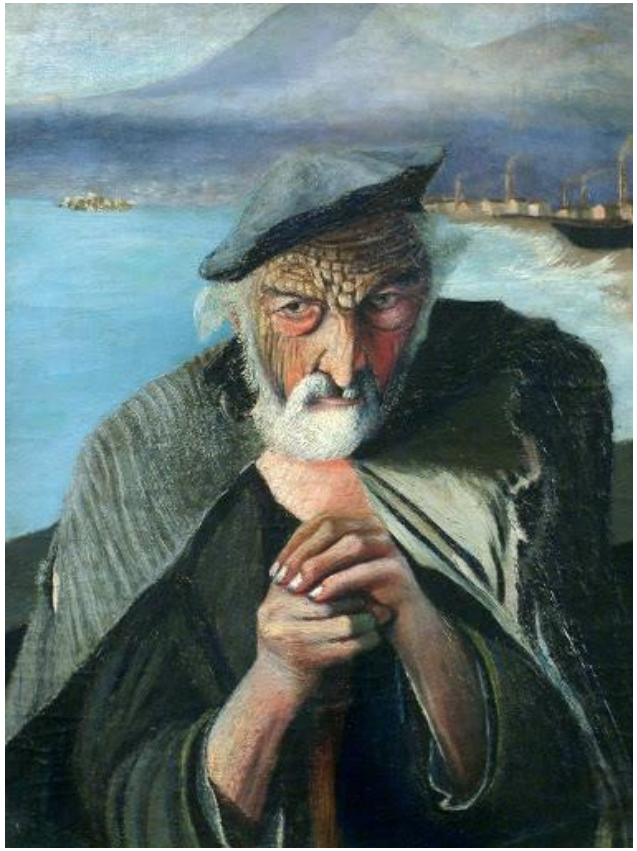



Распределение угроз согласно упоминанию о них в интернет

# НЕМНОГО СВЕЖЕЙ СТАТИСТИКИ.



# СОБИРАЕМСЯ НА РЫБАЛКУ



# ТИПЫ РЫБАЛКИ: ЛОВЛЯ СЕТЬЮ.
## НЕЦЕЛЕВЫЕ АТАКИ

УЛОВ:
- Наибольшее количество данных для дальнейшего анализа и использования.

ВИДЫ РЫБАЦКИХ СЕТЕЙ:
- Электронная почта / web страницы
- Сообщения в мессенджерах / смс
- Голосовые звонки
- Формы авторизации
- Платежные системы

# ТИПЫ РЫБАЛКИ: ЛОВЛЯ СЕТЬЮ.
## НЕЦЕЛЕВЫЕ АТАКИ

**МЕТОДИКА ЗАКИДЫВАНИЯ СЕТЕЙ:**

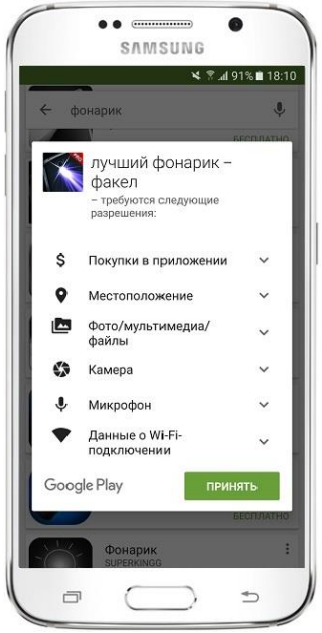
1. СПАМ РАССЫЛКА

- Ссылка на вредоносный сайт (35%)
- Документ со встроенным вредоносным макросом (32%)
- Загружаемый вредоносный код (21%)
- Документ со встроенным вредоносным объектом (12%)

# ТИПЫ РЫБАЛКИ: ЛОВЛЯ СЕТЬЮ.
## НЕЦЕЛЕВЫЕ АТАКИ

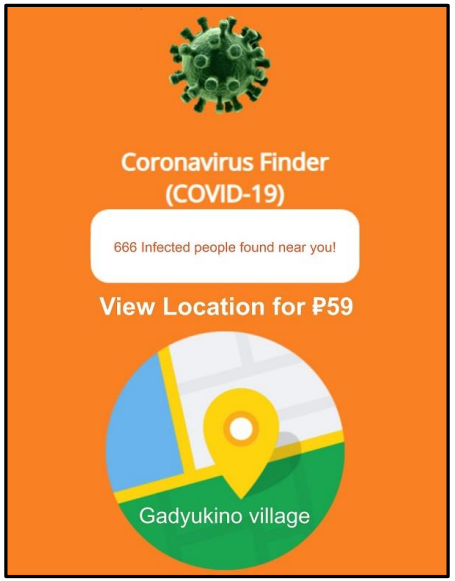
### МЕТОДИКА ЗАКИДЫВАНИЯ СЕТЕЙ:

2. УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ




Очень «любознательное» приложение «Фонарик»
Запрашивает доступ к:
- Данным о WiFi
- Микрофону
- Камере
- Фото/Видео файлам
- Местоположению

….и хочет еще что-то покупать



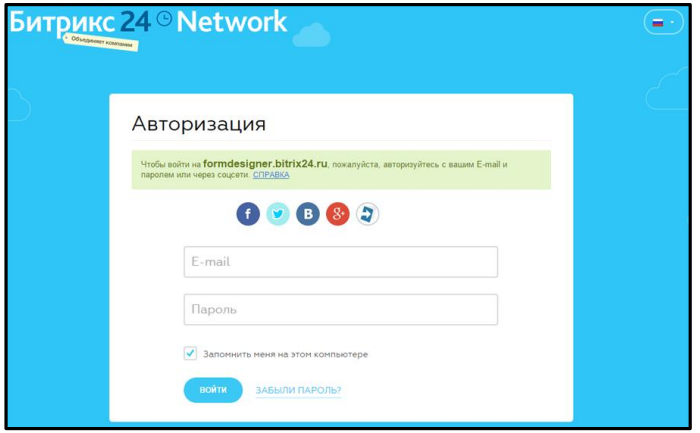

…и конечно же вы захотите узнать кто вокруг вас заражен COVID! И всего за 59р!

# ТИПЫ РЫБАЛКИ: ЛОВЛЯ СЕТЬЮ.
## НЕЦЕЛЕВЫЕ АТАКИ

**МЕТОДИКА ЗАКИДЫВАНИЯ СЕТЕЙ:**

3. ПОСЕЩЕНИЕ ПОДДЕЛЬНЫХ ФОРМ





# ТИПЫ РЫБАЛКИ: ЛОВЛЯ СЕТЬЮ.
## НЕЦЕЛЕВЫЕ АТАКИ

**МЕТОДИКА ЗАКИДЫВАНИЯ СЕТЕЙ:**

4. QR-КОД.

Может вести в полезное место, например на t.me/forensictools

Ну а может:

- Ссылка на вредоносный сайт
- Документ со встроенным вредоносным макросом
- Загружаемый вредоносный код
- Документ со встроенным вредоносным объектом

# ЛУЧШАЯ КОМАНДА «ХАКЕРОВ - СОЦИАЛЬНЫХ ИНЖЕНЕРОВ»

…но как-то отталкивают

# ЛУЧШАЯ КОМАНДА «ХАКЕРОВ - СОЦИАЛЬНЫХ ИНЖЕНЕРОВ»

Фото из ТВ- сериала «Виртуозы» (Ориг. название- Hustle)

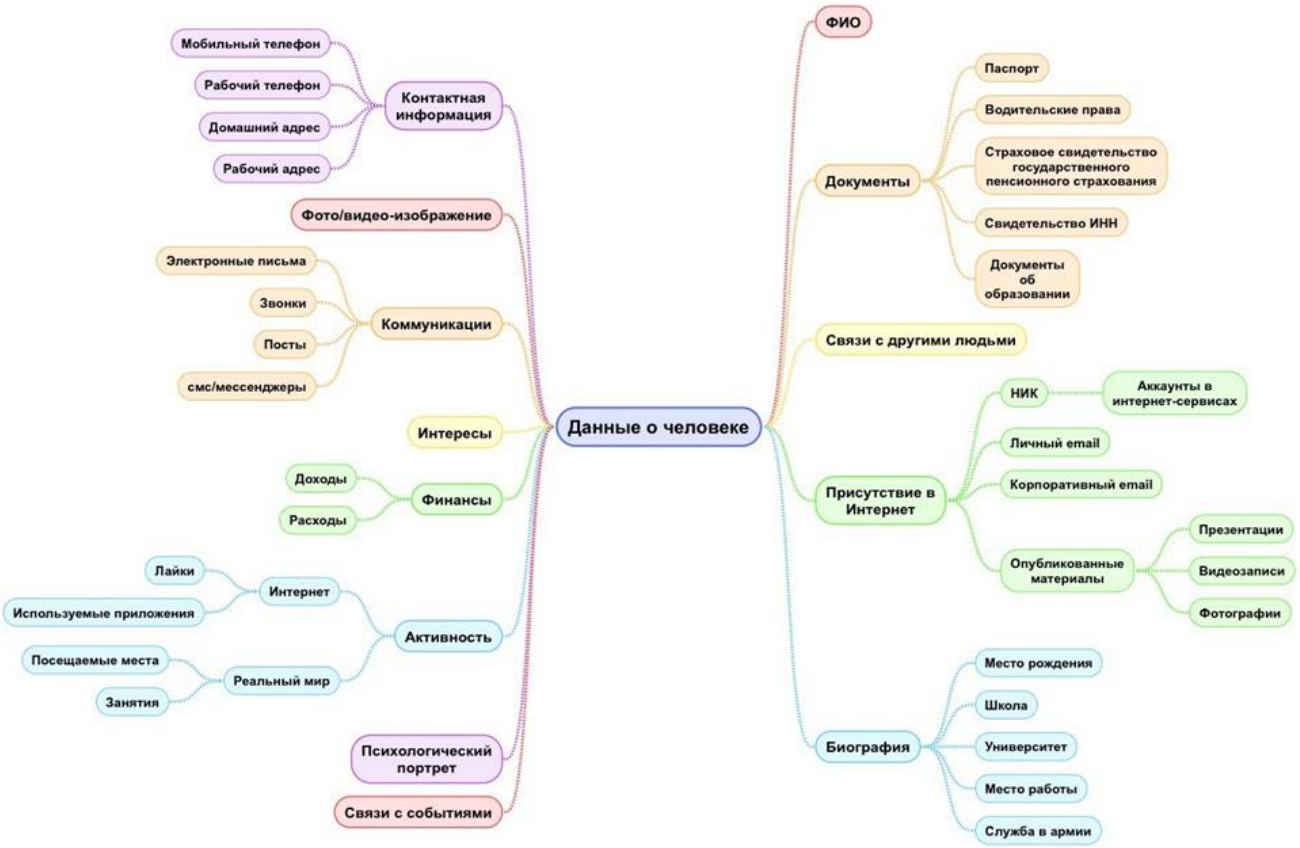
# ТИПЫ РЫБАЛКИ: ЛОВЛЯ УДОЧКОЙ.
## ЦЕЛЕВЫЕ АТАКИ

УЛОВ:
- Данные способные побудить цель совершить необходимые действия личного характера.

ВИДЫ «УДОЧЕК»:
- Электронная почта / web страницы
- Сообщения в мессенджерах / смс
- Голосовые звонки
- Формы авторизации
- Платежные системы
- Социальные сети
- Корпоративные сети

# ТИПЫ РЫБАЛКИ: ЛОВЛЯ УДОЧКОЙ.
## ЦЕЛЕВЫЕ АТАКИ

НАБОР «КРЮЧКОВ»:



# ТИПЫ РЫБАЛКИ: ЛОВЛЯ УДОЧКОЙ.
## ЦЕЛЕВЫЕ АТАКИ

**НАБОР «КРЮЧКОВ»:**

- Место жительства
- Возраст
- Место рождения/работы/учебы/проживания/отдыха
- Имена друзей/коллег/родственников
- Политические/Религиозные взгляды
- Семейное положение
- Взаимоотношения
- Сексуальные предпочтения
- Распространенные имена в социальном окружение;
- Интересы и хобби
- Образ жизни и понятия
- Социальные ценностные факторы

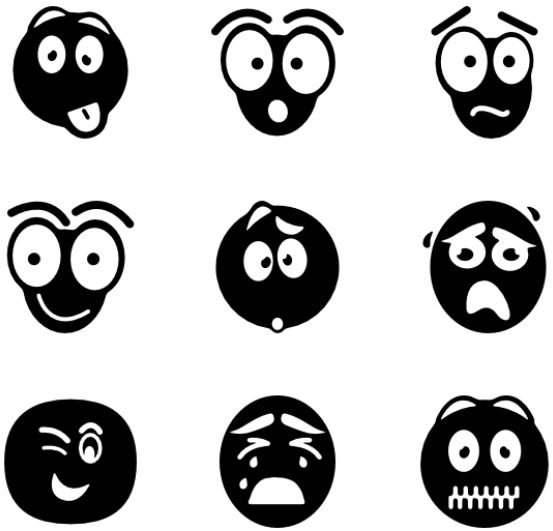
…и многое другое.

# ТИПЫ РЫБАЛКИ: ЛОВЛЯ УДОЧКОЙ.
## ЦЕЛЕВЫЕ АТАКИ

**НАБОР «БЛЁСЕН»:**

ВЫВОД НА ЭМОЦИОНАЛЬНОЕ СОСТОЯНИЕ / ЖЕЛАНИЕ:

- Расположить к себе / Желание помочь
- Показать собственную значимость
- Желание наживы
- Любопытство
- Рассеянность / Невнимательность
- Необходимость срочного принятия решения.
- Раздраженность.
- Усталость



# ТИПЫ РЫБАЛКИ: ЛОВЛЯ УДОЧКОЙ.
## ЦЕЛЕВЫЕ АТАКИ

**НАБОР «НАЖИВКИ»:**

НАЙТИ РЫЧАГ ДАВЛЕНИЯ:

- Компромат:
- Ошибки прошлого
- Наличие тайны
- Стыд

- Манипуляция Эго
- Жадность
- Страх
- Инстинкты

# ИНСТРУМЕНТЫ. «ЧТО В КОРОБКЕ !?»

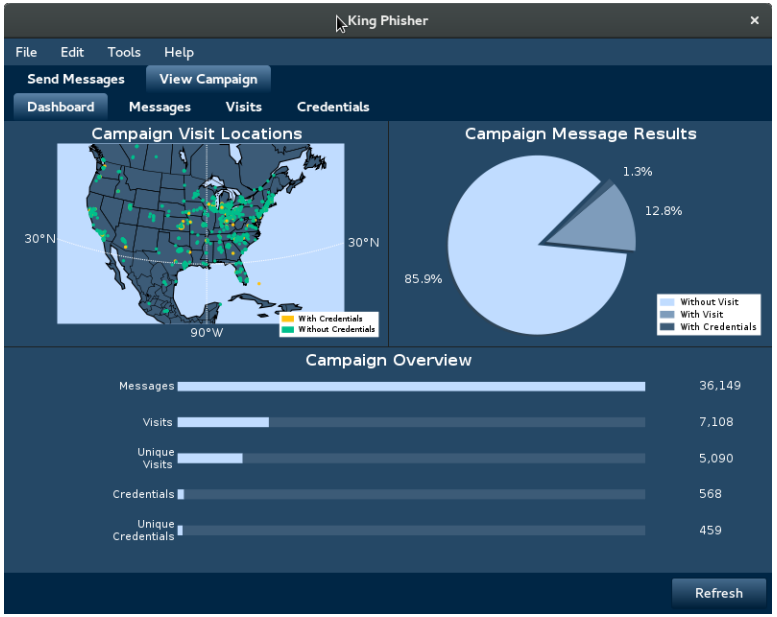
**ИСПОЛЬЗОВАНИЕ МОЖЕТ НАРУШАТЬ ЗАКОН РФ**
**!!!ИСПОЛЬЗОВАТЬ ИСКЛЮЧИТЕЛЬНО В ИССЛЕДОВАТЕЛЬСКИХ ЦЕЛЯХ!!!**

# ФИШИНГ.

Фишинговые атаки компьютер или смартфон субъекта:

KING PHISHER
(github.com/rsmusllp/king-phisher)

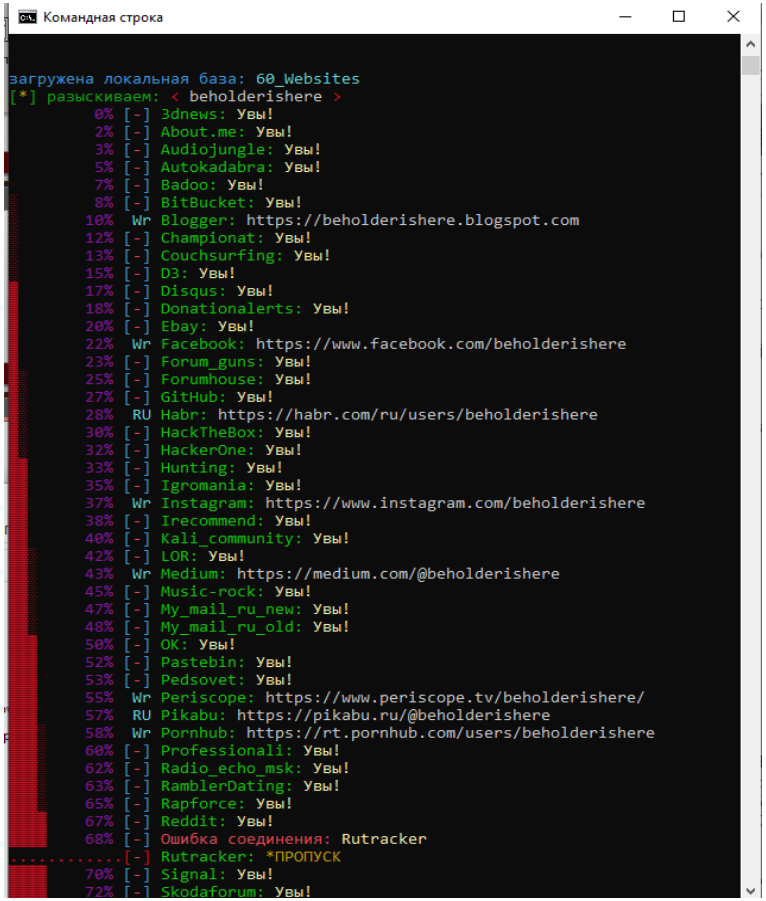
- Запускать одновременно несколько фишинговый атак
- Двухфакторная авторизация
- Собирать учетные данные пользователей с целевых страниц
- Клонировать вебсайты
- Показывать геолокации испытуемых
- Отправлять почту с приглашениями в календари
- Отправлять sms о результатах проведения атак
- Имеет большое количество расширений собственного функционала
- Имеет большое количество настраиваемых шаблонов для имитации страниц и официальных писем.



# OSINT. ИЩЕМ ПО НИКУ ИЛИ ЭЛЕКТРОННОЙ ПОЧТЕ

Ищем по нику в разных сервисах:

- Snoop Project
  https://github.com/snooppr/snoop
- Sherlock Project
  https://github.com/sherlock-project/sherlock



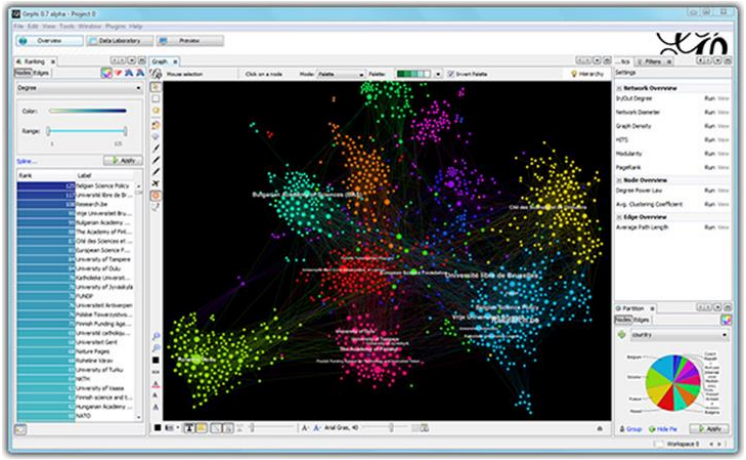
# OSINT. ИЩЕМ СОЦИАЛЬНЫЕ СВЯЗИ

Построение контекстных связей

- Gephi (https://gephi.org/)
- Maltego (https://www.maltego.com)
- Cartography (github.com/lyft/cartography)

Поиск социальных связей:

- YASIV VK (http://yasiv.com/vk)
- Контр.Фокус (http://Focus.kontur.ru)



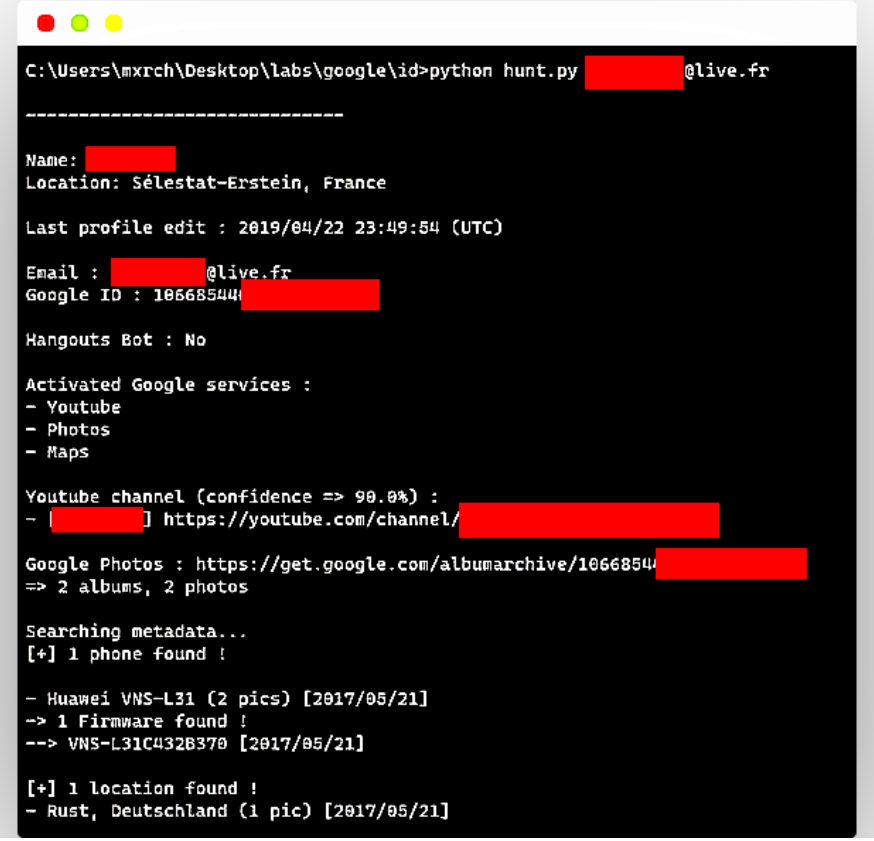
# OSINT. И СНОВА GOOGLE

Все возможные данные из google аккаунта:

GHunt (github.com/mxrch/GHunt)

## Извлекаемые данные:

- Имя владельца
- Последний раз профиль редактировался
- Google ID
- Если это аккаунт Hangouts
- Активированные сервисы Google (Youtube, Фото, Карты, News360, Hangouts и т. Д.)
- Возможный канал Youtube
- Возможные другие имена пользователя
- Публичные фотографии
- Модели телефонов
- Прошивки телефонов
- Установленное ПО
- Обзоры Google Maps
- Возможное физическое местонахождение



**ИСПОЛЬЗОВАНИЕ МОЖЕТ НАРУШАТЬ ЗАКОН РФ !!!ИСПОЛЬЗОВАТЬ ИСКЛЮЧИТЕЛЬНО В ИССЛЕДОВАТЕЛЬСКИХ ЦЕЛЯХ!!!**

# ФИШИНГ.

Фишинговые атаки компьютер или смартфон субъекта:

SEEKER (https://github.com/thewhiteh4t/seeker)

Координаты
Высота
Направление
Скорость
Погрешность

- Operating System
- Platform
- Number of CPU Cores
- Amount of RAM - Approximate Results
- Screen Resolution
- GPU information
- Browser Name and Version
- Public IP Address
- IP Address Reconnaissance

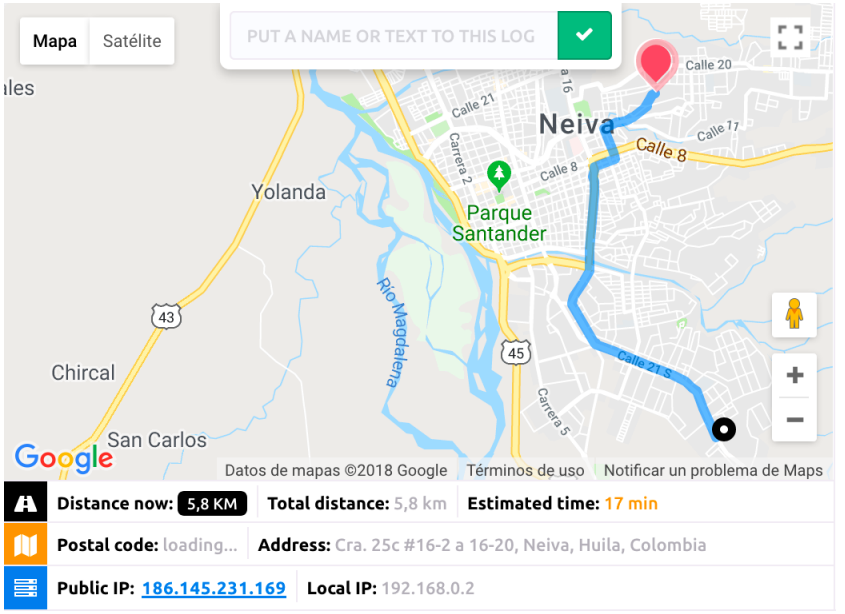
# ФИШИНГ.

**ИСПОЛЬЗОВАНИЕ МОЖЕТ НАРУШАТЬ ЗАКОН РФ !!!ИСПОЛЬЗОВАТЬ ИСКЛЮЧИТЕЛЬНО В ИССЛЕДОВАТЕЛЬСКИХ ЦЕЛЯХ!!!**

Фишинговые атаки компьютер или смартфон субъекта:

TRAPE (https://github.com/jofpin/trape)

- Распознавание сеансов связи с сервисами
- Регистрации в различных сервисах субъектов наблюдения в реальном времени.
- Проведение фишинг-атак в реальном времени
- Картография (координаты и построение путей перемещения)
- Захват различных учетных данных.
- Интеграция с различными OSINT сервисами через открытое API



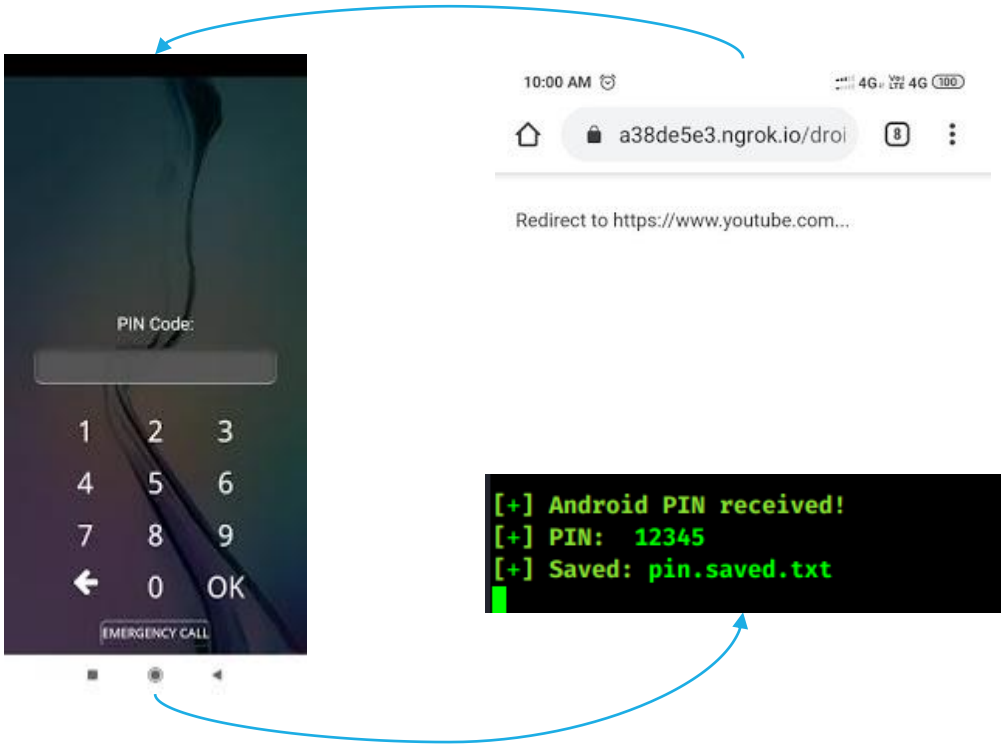
# ФИШИНГ.

**ИСПОЛЬЗОВАНИЕ МОЖЕТ НАРУШАТЬ ЗАКОН РФ**
**!!!ИСПОЛЬЗОВАТЬ ИСКЛЮЧИТЕЛЬНО В ИССЛЕДОВАТЕЛЬСКИХ ЦЕЛЯХ!!!**

Фишинговые атаки компьютер или смартфон субъекта:

LOCKFISH (https://github.com/jaykali/lockphish)

Притворяется экраном блокировки для
- Android
- iOS
- Windows

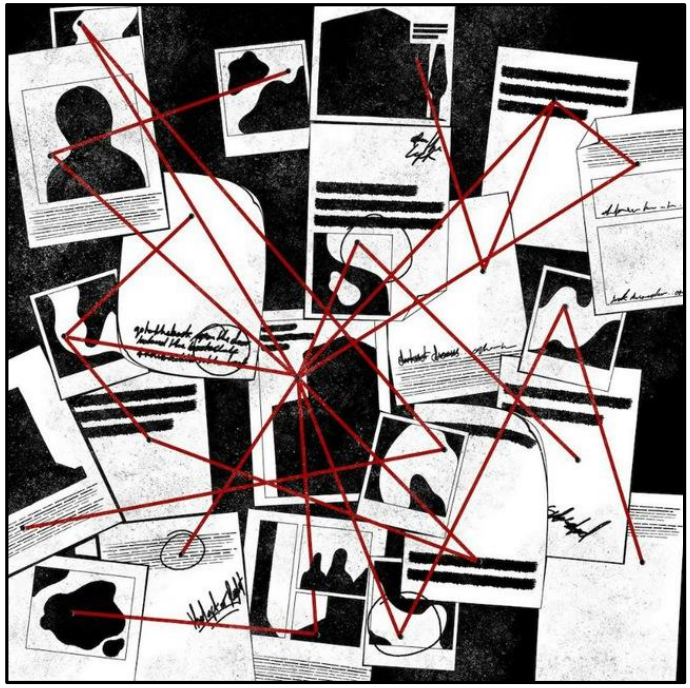



BEHOLDER
IS
HERE

исследования
и консалтинг

**Мой канал в Телеграм:**

## T.ME/ForensicTools



Дмитрий Борощук

Исследования и консалтинг безопасности.

t.me/beholderishere

+7 925 8584075

beholderishere@gmail.com



BEHOLDER
IS
HERE

исследования
и консалтинг