

РЕКЛАМНАЯ РАЗВЕДКА И ДРУГИЕ МЕТОДЫ НАЙТИ ПО МОБИЛЬНИКУ

Игорь Бедеров

Председатель совета по противодействию
технологическим правонарушениям КС НСБ России

Интернет-Розыск (входит в ГК "КИБЕРСИСТЕМА")



Давайте знакомиться!

Российский бизнесмен и общественный деятель. Основатель российской компании «Интернет-Розыск», общественный деятель, изобретатель, популяризатор внедрения инноваций в правоохранительную деятельность. Создатель ряда аналитических продуктов и методик, предназначенных для предупреждения и расследования информационно-телекоммуникационных преступлений.



«Шерлок Холмс цифровой эпохи» – по мнению журнала **RUBEЖ**



Председатель Совета по противодействию технологическим правонарушениям КС НСБ России



Член экспертного совета «International Corporate Security Association» (ICSA)



Советник губернатора Владимирской области



Советник губернатора Вологодской области



Помощник сенатора Российской Федерации



Эксперт инжинирингового центра «SafeNet» Национальной технологической инициативы (НТИ) 20.35



Член правления Федерации Спортивного Программирования Санкт-Петербурга



Сооснователь клуба руководителей служб безопасности «СБ-Питер»



Основатель компании «Интернет-Розыск» (входит в ГК «Киберсистема»)



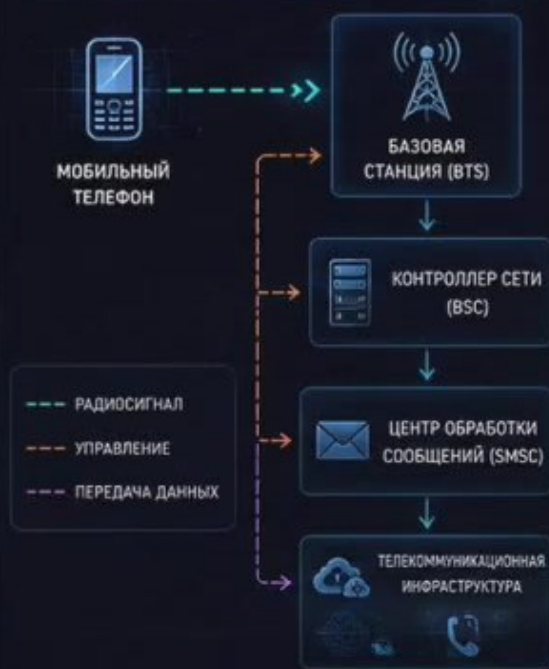
**ИГОРЬ
БЕДЕРОВ**



ЭВОЛЮЦИЯ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ В GSM-СЕТЯХ

От крупных зон покрытия к точным координатам

АРХИТЕКТУРА МОБИЛЬНОЙ СЕТИ (2010-Е)



ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ПО СЕТИ GSM



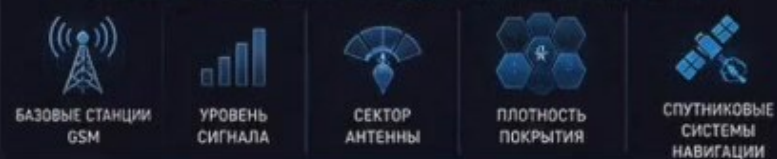
ПРОЦЕСС УТОЧНЕНИЯ ПОЛОЖЕНИЯ



ЭВОЛЮЦИЯ ТЕХНОЛОГИЙ ГЕОЛОКАЦИИ



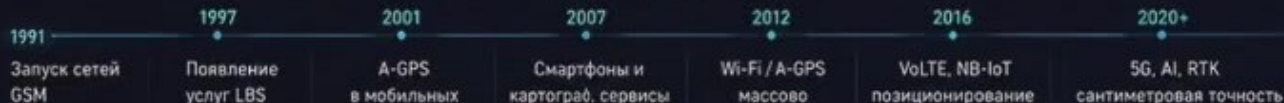
ОСНОВНЫЕ ИСТОЧНИКИ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ



РОСТ ТОЧНОСТИ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ



КЛЮЧЕВЫЕ ВЕХИ РАЗВИТИЯ



СЛЕЖКА ЗА МОБИЛЬНЫМ УСТРОЙСТВОМ



Вопрос отслеживания местоположения мобильного устройства — один из самых частых в практике OSINT-специалиста.



Причины могут быть разными: от поиска потерянного телефона родственника до проверки гипотез в рамках расследования.



Важно сразу оговориться: все методы требуют законных оснований для применения и глубокого понимания этических норм.

Несанкционированное слежение является уголовным преступлением.



МЕТОДЫ ОРГАНИЗАЦИИ СЛЕЖКИ ЗА МОБИЛЬНИКОМ РАЗДЕЛЯЮТСЯ НА ДВЕ КАТЕГОРИИ:



БЕЗ ДОСТУПА К УСТРОЙСТВУ

Методы, позволяющие получить информацию о местоположении устройства удалённо, без физического взаимодействия с ним.

VS

С ДОСТУПОМ К УСТРОЙСТВУ

Методы, требующие разблокированного устройства для установки инструментов, изменения настроек или извлечения данных.



Все действия должны осуществляться исключительно в рамках закона и с соблюдением этических норм.
Несанкционированное слежение является уголовным преступлением.





КОГДА ДОСТУП К ТЕЛЕФОНУ ВОЗМОЖЕН

1 ПО ДЛЯ РОДИТЕЛЬСКОГО КОНТРОЛЯ

После однократной физической установки и настройки на целевом устройстве приложение предоставляет удаленный доступ к данным.



Местоположение
в реальном времени



История
перемещений



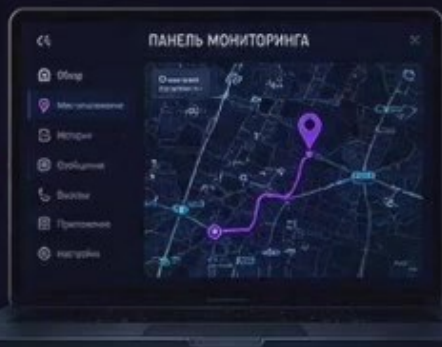
Сообщения
и мессенджеры



Вызовы и
контакты



Другие
данные



Работает
скрытно



Круглосуточный
мониторинг



Данные в
облаке



Мгновенные
уведомления



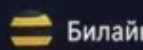
Изначально создано для защиты детей,
может применяться для мониторинга взрослых
с их согласия и в рамках закона.

2 УСЛУГИ ОПЕРАТОРА СВЯЗИ

Использование штатных платных услуг операторов сотовой связи: «Локатор» или «Геопоиск».



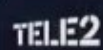
MTS



Билайн



МегаФон



TELE2

Технологии определения местоположения.



LBS
(Location-based service)
определение по данным
сети оператора



Триангуляция
определение по сигналам
между вышками
сотовой связи



Высокая
точность



Работает без
установки ПО



Легально через
оператора



Точность зависит от плотности покрытия сети
и может достигать 10–100 метров
в городских условиях.

3 ТРАНСЛЯЦИЯ ГЕОПОЗИЦИИ

Активация функции «Поделиться геопозицией» в популярных мессенджерах и картографических сервисах.



Telegram



Google Maps

Другие
сервисы



Выбор
контакта



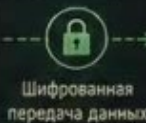
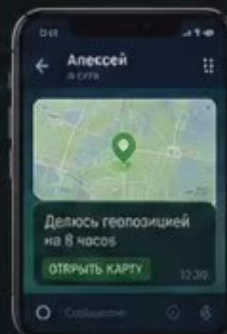
Активация
геопозиции



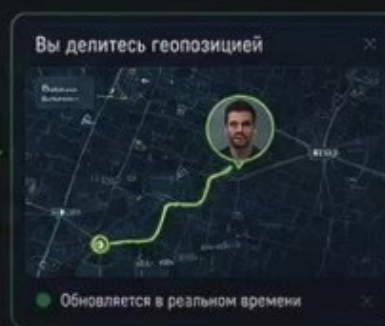
Выбор
периода



Передача
координат



Шифрованная
передача данных



Реальное время



Контроль доступа
(кому и на какой срок)



Прозрачно для
пользователя



Работает только при согласии владельца устройства.
Просто, быстро и удобно.



ДОСТУП К МЕСТОПОЛОЖЕНИЮ СТАНОВИТСЯ ВОЗМОЖНЫМ ТОЛЬКО ПРИ ФИЗИЧЕСКОМ ДОСТУПЕ К УСТРОЙСТВУ ИЛИ СОГЛАСИИ ВЛАДЕЛЬЦА.

Используйте только законные методы и уважайте частную жизнь.





Для OSINT-специалиста заблокированный смартфон — **не тупик, а вызов.**

Расследования, где критически важна информация с телефона (от предотвращения преступлений до поиска пропавших людей), требуют умения обходить защиту.



Экран блокировки не просто мешает доступу — он блокирует ключевые функции.



Однако техника часто уступает психологии.



ПРЕДУПРЕЖДЕНИЕ:

Несанкционированный взлом устройств преследуется по закону.



СПОСОБЫ ПОЛУЧЕНИЯ ДОСТУПА: **ЧЕЛОВЕЧЕСКИЙ ФАКТОР И ТЕХНИКИ**



- **70%** владельцев охотно сообщают код, особенно если это ускорит возврат устройства.



- **Физический захват** телефона в момент его разблокировки. Схожим образом работает и просьба "дать позвонить".



- **Наблюдение за вводом кода** (лично или через камеры видеонаблюдения).



- **Поиск записей в блокнотах, под чехлом, в облаке, утечках.** **26.83%** паролей покрываются 20 комбинациями (1234, 1111, 0000). Простые геометрические фигуры (буквы, углы) угадываются с первых попыток.



- **Обработка экрана порошком** (даже детской присыпкой) выявляет следы пальцев. Анализ следов и знание привычек владельца приводят к сужению круга вариантов.

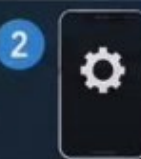


- **3D-копия отпечатка или маска лица** (фото на 5-литровой банке) обманывают биометрию. Старые сканеры уязвимы к фото, современные (FaceID, ультразвуковые датчики) сложнее, но не неуязвимы.

ДОСТУП ЧЕРЕЗ SIM-КАРТУ В РАЗБЛОКИРОВАННОМ УСТРОЙСТВЕ



1
Физически выньте SIM-карту из заблокированного устройства.



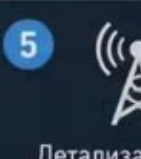
2
Убедитесь, что SIM не защищена PIN-кодом.



3
Вставьте SIM в разблокированный смартфон с чистым состоянием ОС.



4
Активируйте мобильный интернет и восстановите доступ к нужным аккаунтам (функция "Забыли пароль?").



5
Детализацию GSM-соединений вы сможете выгрузить в личном кабинете оператора связи.



6
А перемещения — через сервисы Android или iOS.



Законность и этика: все действия должны выполняться исключительно в рамках закона и с соответствующими полномочиями.

БЕЗ ПРЯМОГО ДОСТУПА К ЦЕЛЕВОМУ УСТРОЙСТВУ

ЭТИ МЕТОДЫ ОСНОВАНЫ НА УДАЛЕННОМ ВЗАИМОДЕЙСТВИИ С ЦЕЛЬЮ ИЛИ ЭКСПЛУАТАЦИИ РАЗЛИЧНЫХ ЦИФРОВЫХ СЕРВИСОВ.



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Самый недооцененный, но зачастую чрезвычайно эффективный метод.

ВОЗМОЖНЫЕ ЛЕГЕНДЫ



Сотрудник банка
«Служба безопасности»



Служба доставки
«Уточнение адреса»



Техническая поддержка
«Решение проблемы»



Государственный орган
«Официальный запрос»



Не взлом устройства,
а взлом человека.

Психология, доверие, правдоподобие.



УДАЛЕННОЕ ВЗАИМОДЕЙСТВИЕ
БЕЗ ФИЗИЧЕСКОГО ДОСТУПА

ЦЕЛЬ

Здравствуйте!
Вас беспокоит служба
безопасности банка...

Нам нужно уточнить
некоторые данные
для вашей защиты.

Это займет всего
несколько минут.



ДОВЕРИЕ
И УБЕЖДЕНИЕ



ТЩАТЕЛЬНЫЙ АНАЛИЗ ОТКРЫТЫХ ПРОФИЛЕЙ И ИХ УПОМИНАНИЙ
ЧАСТО ВЫДАЕТ НЕ ТОЛЬКО ГОРОД, НО И ЛЮБИМЫЕ КАФЕ,
МАРШРУТЫ И МЕСТО РАБОТЫ.

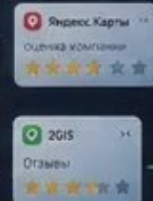


АНАЛИЗ ОТКРЫТЫХ ИСТОЧНИКОВ

Анализ геометок в соцсетях и публичных карт.
Открытые профили выдают больше, чем кажется.

ИСТОЧНИКИ ДАННЫХ

- Социальные сети
- Публикации и фото
- Геометки и чекины
- Отзывы и комментарии
- Публичные карты
- Профили и резюме



ЦИФРОВОЙ СЛЕД



ЦИФРОВОЙ ПРОФИЛЬ

- ИНТЕРЕСЫ
- ПРИБЫЧКИ
- РАСПИСАНИЕ
- СОЦИАЛЬНЫЕ СВЯЗИ
- МЕСТОПОЛОЖЕНИЕ

1

ОТКРЫТЫЕ ДАННЫЕ

Сбор информации из доступных источников (соцсети, карты, форумы, отзывы, чаты и др.)



2

АНАЛИЗ ПОВЕДЕНИЯ

Выявление паттернов, привычек, интересов, маршрутов и связей цели.



3

ФОРМИРОВАНИЕ ЛЕГЕНДЫ

Создание убедительной легенды под контекст цели и выбор канала коммуникации.



4

КОНТАКТ С ЦЕЛЬЮ

Установление контакта под легендой и выстраивание доверия для получения нужной информации.



5

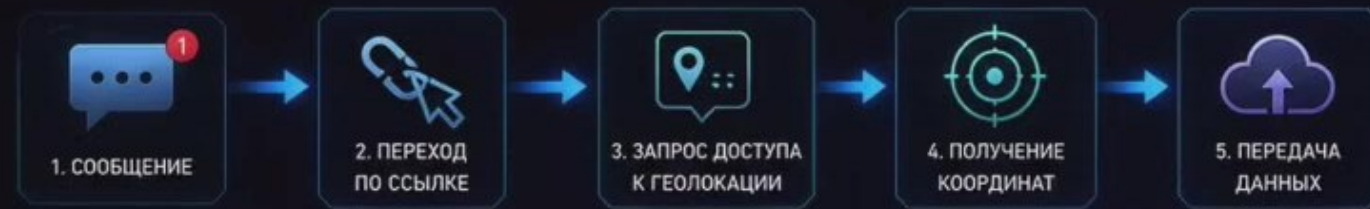
ПОЛУЧЕНИЕ ИНФОРМАЦИИ

Добыча нужных данных: доступы, документы, местоположение и др.



Все методы требуют законных оснований для применения и глубокого понимания этических норм.
Несанкционированное слежение является уголовным преступлением.





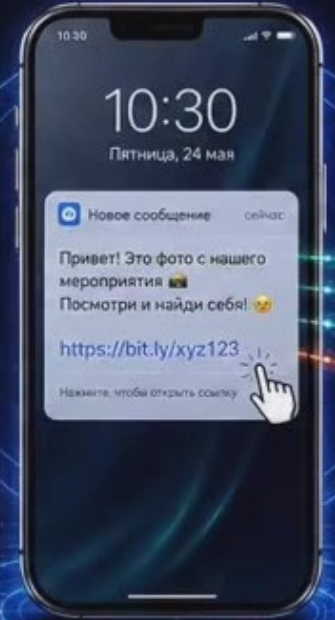
КАНАЛЫ ДОСТАВКИ

- ЭЛЕКТРОННАЯ ПОЧТА
- МЕССЕНДЖЕР
- SMS
- СОЦИАЛЬНАЯ СЕТЬ

МАСКИРОВАННАЯ ССЫЛКА

<https://bit.ly/xyz123>

- НОВОСТЬ
- ДОКУМЕНТ
- ПРИГЛАШЕНИЕ НА МЕРОПРИЯТИЕ
- УВЕДОМЛЕНИЕ О ДОСТАВКЕ



ГЕОЛОГЕРЫ (ПРИМЕРЫ)

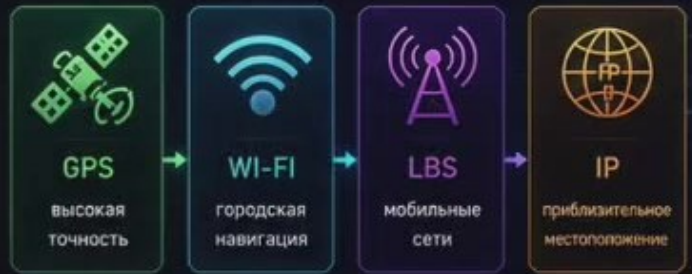
- github.com/thewhiteh4t/seeker
- github.com/jofpin/trape
- github.com/cryptomarauder/TrackUrl
- github.com/Bafomet666/Bigbro
- github.com/spyboy-productions/r4ven
- iplogger.org/location-tracker/



ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ



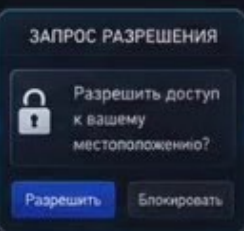
HTML5 GEO API



HTML5 Geo API



БРАУЗЕР ПОЛЬЗОВАТЕЛЯ



ЗАПРОС РАЗРЕШЕНИЯ

Разрешить доступ к вашему местоположению?

Разрешить | Блокировать

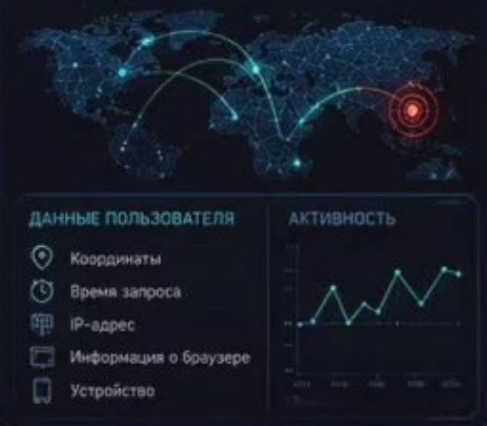


КООРДИНАТЫ



УДАЛЁННЫЙ ВЕБ-РЕСУРС

ПЕРЕДАЧА ДАННЫХ



ПЕРЕДАЧА ДАННЫХ

SYSTEM STATUS
SECURE CONNECTION
ACTIVE



Email

Пароль

ДОСТУП К УСТРОЙСТВУ



СЕРВИСЫ ПОИСКА УСТРОЙСТВ

Устройство найдено
Точность: 10 м

ПОИСК УСТРОЙСТВА
Определение местоположения на карте

УДАЛЕННАЯ БЛОКИРОВКА
Блокировка устройства удаленно

ПОДАЧА СИГНАЛА
Воспроизведение звукового сигнала на устройстве

ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ



УГРОЗЫ БЕЗОПАСНОСТИ АККАУНТА

УЧЕТНАЯ ЗАПИСЬ

fingerprint.to
Digital Footprint

УТЕЧКА ДАННЫХ

osintleak.com
OSINT Data

КОМПРОМЕТАЦИЯ ДОСТУПА

hudsonrock.com
Breach Intelligence

УТЕЧКИ И ПОДБОР ПАРОЛЕЙ

leakradar.io
Leak Monitoring

⚠️ РИСК ПОТЕРИ ДОСТУПА К УСТРОЙСТВУ И ДАННЫМ

GLOBAL NETWORK
CONNECTED DEVICES
128.7M

Email

Пароль

• • • • •

ДЛЯ ДОСТУПА К ЛОКАЦИИ УСТРОЙСТВА
ТРЕБУЕТСЯ АВТОРИЗАЦИЯ В УЧЕТНОЙ ЗАПИСИ
(EMAIL + ПАРОЛЬ), К КОТОРОЙ ОНО ПРИВЯЗАНО.



ВАШ СМАРТФОН ПОСТОЯННО СООБЩАЕТ МИРУ О СВОЕМ МЕСТОПОЛОЖЕНИИ

И для прослушивания этого сигнала не нужен хакерский талант — достаточно бесплатного приложения.



Wigle

Глобальная база данных точек доступа и вышек сотовой связи. Люди со всего мира загружают сюда результаты сканирования Wi-Fi и Bluetooth.



nRF Connect

Профессиональный инструмент для разработчиков Bluetooth-устройств, ставший стандартом для мониторинга BLE-трафика.



LightBlue Explorer

Аналог nRF Connect для iOS и macOS. Удобный интерфейс, быстрое сканирование, возможность подключения к BLE-устройствам для изучения их характеристик.



BLE Radar

Специализированная утилита, которая визуализирует устройства в пространстве в реальном времени, оценивая расстояние по мощности сигнала.



ВАШ СМАРТФОН — ПЕРЕДАТЧИК ИДЕНТИФИКАТОРОВ



КАК ЭТО РАБОТАЕТ



1. СМАРТФОНЫ
ПЕРЕДАЮТ
BLE-СИГНАЛЫ



2. ПРИЛОЖЕНИЕ
СКАНИРУЕТ
ОКРУЖЕНИЕ



3. ОПРЕДЕЛЯЕТ
УСТРОЙСТВА
И РАССТОЯНИЯ



4. ОТОБРАЖАЕТ
НА КАРТЕ
В РЕАЛЬНОМ ВРЕМЕНИ

РЕАЛЬНОЕ ВРЕМЯ: КАРТА ОБНАРУЖЕННЫХ УСТРОЙСТВ

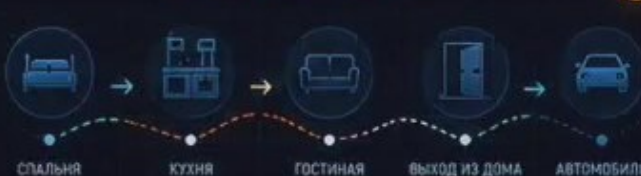
- iPhone 15 Pro 12 m
- AirPods Pro 18 m
- Galaxy S23 24 m
- Apple Watch 31 m
- MacBook Air 45 m
- Fitbit Sense 2 56 m



ЧТО ВЫ ВИДИТЕ ЧЕРЕЗ 30 СЕКУНД

- ТОЧНЫЕ МОДЕЛИ УСТРОЙСТВ (iPhone 15 Pro, Samsung Galaxy S23, AirPods Pro и др.)
- РАССТОЯНИЕ ДО НИХ С УДИВИТЕЛЬНОЙ ТОЧНОСТЬЮ
- ИХ КООРДИНАТЫ НА КАРТЕ

ПРИМЕР НАБЛЮДЕНИЯ



ВЫ В РЕАЛЬНОМ ВРЕМЕНИ НАБЛЮДАЕТЕ ЗА ПЕРЕМЕЩЕНИЕМ ЦИФРОВЫХ «ПРИЗРАКОВ» ВАШИХ СОСЕДЕЙ, КОЛЛЕГ, ПРОХОЖИХ.



РИСКИ ДЛЯ КОНФИДЕНЦИАЛЬНОСТИ



ПАССИВНОЕ
ОТСЛЕЖИВАНИЕ
ПЕРЕМЕЩЕНИЙ



ПРОФИЛИРОВАНИЕ
И ПОВЕДЕНЧЕСКИЙ
АНАЛИЗ



ДЕАНОНИМИЗАЦИЯ
УСТРОЙСТВ
И ПОЛЬЗОВАТЕЛЕЙ



УТЕЧКА ДАННЫХ
О ПРИСУТСТВИИ
И АКТИВНОСТИ

ЭВОЛЮЦИЯ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ



ИСТОЧНИКИ ДАННЫХ О МЕСТОПОЛОЖЕНИИ



BLUETOOTH-ТРЕКЕРЫ против «НЕВИННОГО» НАУШНИКА

ОДИН МАЛЕНЬКИЙ ДЕВАЙС — ДВА СЦЕНАРИЯ. КАК ЛЕГКО ОСТАТЬСЯ НЕЗАМЕЧЕННЫМ.

BLUETOOTH-ТРЕКЕРЫ: УДОБСТВО И РИСКИ



AirTag



Tile

УЯЗВИМОСТИ ТРЕКЕРОВ



iOS и Android предупреждают об обнаружении неопознанных трекеров



Множество приложений сканируют эфир на предмет сигналов трекеров



Трекер можно обнаружить визуально при внимательном осмотре

ПРИМЕРЫ ПРИЛОЖЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ



Tracker Detect
(Android & iOS)



DontTrack
(Android)



AirGuard
(iOS)



BLE Scanner
(Android)

ДВА УСТРОЙСТВА. ДВА ВОСПРИЯТИЯ.



ПОДОЗРИТЕЛЬНО

- Трекер = устройство слежения
- Вызывает настороженность
- Высокий риск обнаружения

VS



ОБЫДЕННО

- Наушник = потеря/находка
- Не вызывает подозрений
- Низкий риск обнаружения

ВОЗМОЖНЫЕ МЕСТА «СЛУЧАЙНОЙ ПОТЕРИ» НАУШНИКА



СУМКА



ПОД СИДЕНЬЕМ
МАШИНЫ



КАРМАН
КУРТКИ



ОФИС / ДОМ



РАЗДЕВАЛКА /
СПОРТЗАЛ

РЕАКЦИЯ ЧЕЛОВЕКА НА НАХОДКУ НАУШНИКА



ОЙ, КТО-ТО ПОТЕРЯЛ
НАУШНИК!



ВЫКИНУТЬ? ИЛИ МОЖЕТ,
ПРИГОДИТСЯ?

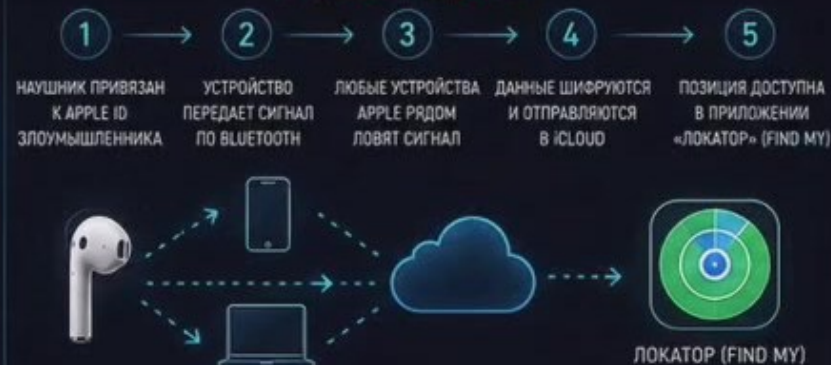


ПОПРОБУЮ ПОДКЛЮЧИТЬ
(НЕ ВСЕГДА УДАЧНО)



ОСТАВИТ НА ВИДНОМ
МЕСТЕ ИЛИ У СЕБЯ

КАК РАБОТАЕТ ОТСЛЕЖИВАНИЕ НАУШНИКА В ЭКОСИСТЕМЕ APPLE



ПРЕИМУЩЕСТВА НАУШНИКА КАК ТРЕКЕРА



Маленький
и незаметный



Обычный аксессуар,
не вызывает подозрений



Сложно
обнаружить
сканерами



Встроен в экосистему
Apple (точное
отслеживание)

КАРТА ПЕРЕМЕЩЕНИЙ (ПРИМЕР)



ВАЖНО ПОМНИТЬ

Использование чужих устройств для скрытого отслеживания может являться нарушением закона и прав человека. Данный материал носит исключительно информационный характер для повышения осведомлённости о рисках.



ИСТОЧНИКИ РЕКЛАМНЫХ ДАННЫХ

1 ПОИСКОВЫЕ ПЛАТФОРМЫ



- АУДИТОРИИ
- РЕКЛАМНЫЕ СЕГМЕНТЫ
- АНАЛИТИКА
- СТАТИСТИКА ВЗАИМОДЕЙСТВИЙ
- ОБЪЕДИНЕННЫЕ ДАННЫЕ



2 СОЦИАЛЬНЫЕ СЕТИ



- АУДИТОРИИ
- РЕКЛАМНЫЕ СЕГМЕНТЫ
- АНАЛИТИКА
- СТАТИСТИКА ВЗАИМОДЕЙСТВИЙ
- ОБЪЕДИНЕННЫЕ ДАННЫЕ



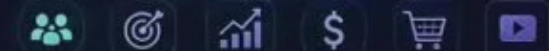
3 ТЕЛЕКОММУНИКАЦИОННЫЕ ОПЕРАТОРЫ



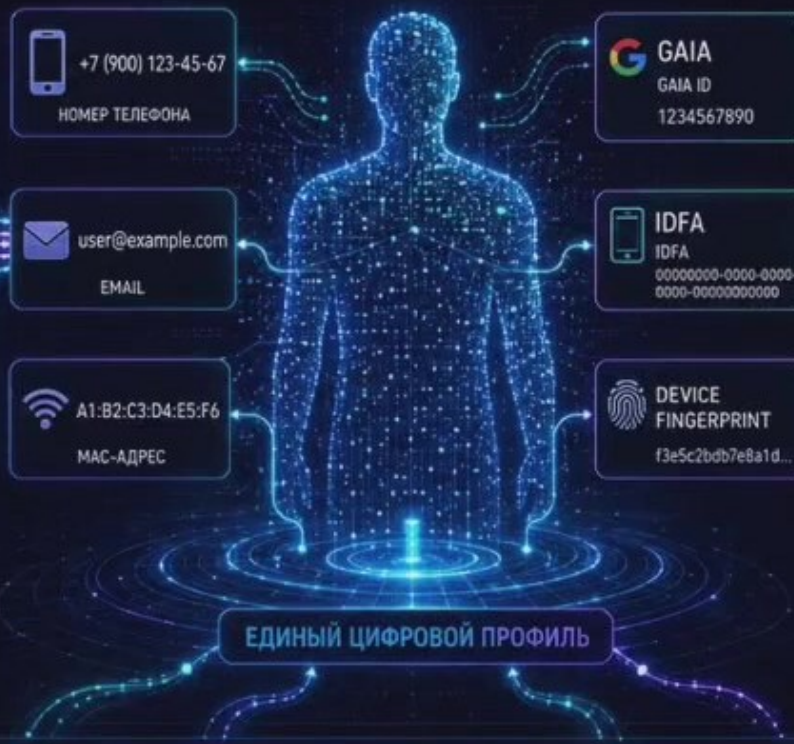
- АУДИТОРИИ
- РЕКЛАМНЫЕ СЕГМЕНТЫ
- АНАЛИТИКА
- СТАТИСТИКА ВЗАИМОДЕЙСТВИЙ
- ОБЪЕДИНЕННЫЕ ДАННЫЕ



ЕДИНАЯ РЕКЛАМНАЯ ЭКОСИСТЕМА



ADINT (Advertising Intelligence)



ГЕОГРАФИЧЕСКАЯ АНАЛИТИКА



ГЕОЗОНЫ

- ЗОНА А
- ЗОНА В
- ЗОНА С
- ЗОНА D

УСТРОЙСТВА

12 589
АКТИВНЫХ УСТРОЙСТВ

СИГНАЛЫ

24 786
СОБЫТИЙ

ВРЕМЕННЫЕ МЕТКИ

- 10:15 - Активность
- 10:27 - просмотр рекламы
- 10:42 - клик по объявлению
- 11:03 - посещение локации

АНАЛИТИЧЕСКИЕ МАРКЕРЫ

- Точки интереса
- Аноним передвижений
- Частота посещений
- Взаимодействие с рекламой

АКТИВНОСТЬ ПО ВРЕМЕНИ



ПОСЕЩАЕМОСТЬ ЗОН



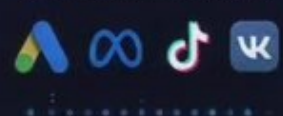
ТИПЫ УСТРОЙСТВ



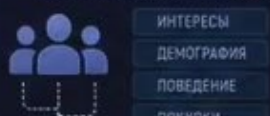
1. ИДЕНТИФИКАТОРЫ



2. РЕКЛАМНЫЕ ПЛАТФОРМЫ



3. АУДИТОРНЫЕ СЕГМЕНТЫ



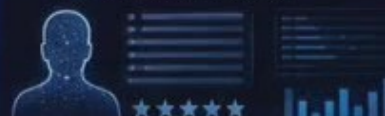
4. ГЕОАНАЛИТИКА



5. ПОВЕДЕНЧЕСКИЕ МОДЕЛИ



6. ЦИФРОВОЙ ПРОФИЛЬ



ВОЗМОЖНОСТИ РЕКЛАМНЫХ ДАННЫХ

СОЗДАНИЕ СОЦИАЛЬНОГО ПОРТРЕТА ПОЛЬЗОВАТЕЛЯ ИЛИ ГРУППЫ ЛИЦ



ОТСЛЕЖИВАНИЕ ИЛИ КОНТРОЛЬ ПЕРЕМЕЩЕНИЙ



ВЫЯВЛЕНИЕ СОЦИАЛЬНЫХ СВЯЗЕЙ И КОНТАКТОВ



СБОР ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ В ЗАДАННОЙ МЕСТНОСТИ



НАВЕДЕНИЕ ВЫСОКОТОЧНОГО ОРУЖИЯ



ДОСТАВКА И УСТАНОВКА ШПИОНСКОГО ПО



LIVE DATA STREAM



Осло Выберите свой город

20 °C
CORRELATION
ATTRIBUTION
REPORTING

- ТЕЛЕФОН
 - HLR, PING, РЕГИСТРАЦИЯ
 - ПОИСК РЕГИСТРАЦИЙ
 - УТЕЧКИ
 - БИЛЛИНГ И ДЕТАЛИЗАЦИЯ
- EMAIL
 - ПОИСК УСТРОЙСТВА
 - ГЕОЛОГИРОВАНИЕ
 - ADINT
- ГЕОЛОКАЦИЯ
 - ПОИСК УСТРОЙСТВА
 - ГЕОЛОГИРОВАНИЕ
 - ADINT
- БАЗОВЫЕ СТАНЦИИ
- IMEI

- IPLOGGER [HTML5 GEO]
- RAVEN [HTML5 GEO]
- BIGBRO [HTML5 GEO]
- TRACKURL [HTML5 GEO]
- TRAPE [HTML5 GEO]
- SEEKER [HTML5 GEO]
- NGROK [HTML5 GEO]

OSINTbro

FIND THE TRUTH. CONNECT THE DOTS.



СКАЧАТЬ

Case #2701
Digital Footprint

- WHO
- WHAT
- WHERE
- WHEN
- WHY
- HOW

MATCH FOUND



ВИЗИТКА

