Разведка по открытым источникам

OSINT. Кибербразведка. Конкурентный анализ. Социальная инженерия

OSINT/кибербразведка/социальная инженерия

Open source intelligence (OSINT) - разведка по открытым источникам, которая заключается в поиске, выборе, сборе и анализе разведывательной информации из общедоступных источников.

Кибербразведка - это знание и понимание злоумышленников и их вредоносных активностей, позволяющее защищающимся и их организациям минимизировать ущерб за счет принятия более эффективных решений в области безопасности.

Социальная инженерия (СИ) / Social engineering (SE) - совокупность приёмов, методов и технологий формирования условий и обстоятельств, которые максимально эффективно приводят к необходимому результату с использованием социологии и психологии.

Виды OSINT

Виды OSINT

Пассивный

Пассивный тип проведения сбора и анализа данных состоит в том, что объект исследования не сможет определить, что о нём собирается информация. Поиск ограничивается контентом на сайте объекта исследования, архивной информацией, незащищенными файлами или же на смежных с объектом ресурсах.

Виды OSINT

Активный

Активный же тип OSINT’а предполагает активное взаимодействие с объектом исследования. К такому типу может относиться: получение доступа к открытым портам, сканирование уязвимостей и серверных веб-приложений, социальная инженерия. Однако у данного типа есть минус: объект сможет обнаружить факт исследований.

Виды OSINT

Полупассивный

пытается имитировать типичный интернет-трафик, что позволяет производить разведку скрытно, не привлекая внимания неординарным поведением.

Виды OSINT

Деанонимизация - самый распространённый вид. Заключается в установлении личности человека.

Доксинг – разновидность деанона, заключающаяся в публикации данных, с целью мести.

Конкурентная разведка — это деятельность компании, которая подразумевает сбор и анализ информации о конкурентах, конкурентоспособных продуктах и услугах. Вся информационно-аналитическая работа проводится исключительно в рамках этических норм.

Кто пользуется OSINT

- **Правительство** - государственные органы, особенно военные ведомства, считаются крупнейшим потребителем источников OSINT.
  Правительствам нужны источники OSINT для различных целей, таких как национальная безопасность, кибер-слежка за террористами, понимание взглядов отечественной и зарубежной общественности по различным вопросам и другие.
- **Международные организации -** Международные организации, такие как ООН, используют источники OSINT для поддержки миротворческих операций.
- **Гуманитарные организации** - используют источники OSINT, чтобы помочь им в их усилиях по оказанию помощи во время кризиса или катастрофы и других целей.
- **Правоохранительные органы** - полиция использует источники OSINT для защиты граждан от преступлений.
- **Бизнес-корпорации** - корпорации используют источники OSINT для исследования новых рынков, мониторинга деятельности конкурентов, планирования маркетинговой деятельности и другого.
- **Частные Лица** – используют OSINT для мести, проверки на измену, поиска пропавшего родственника и другого.

Источники данных

- публикации в СМИ, научных изданиях, доклады на конференциях
- посты и комментарии в социальных сетях
- документы из открытых архивов, публичные данные из государственных информационных систем, судебная информация
- публичные коммерческие данные (выручка, прибыль, стоимость акций)
- данные о структуре и сотрудниках компаний с их сайтов и страниц в социальных сетях
- слитые базы

Характеристики информации

Доронин А. Бизнес-разведка

Критерии оценки информации

1 Объективность – необъективность
объективная информация максимально очищена от мнений, оценок, суждений

2 Достоверность – недостоверность
достоверная информация отражает истинное положение дел

3 Полнота – неполнота
если информация полна, то ее достаточно для принятия правильного решения

4 Актуальность – неактуальность
ценность информации резко падает со временем

5 Ценность – бесполезность
информация полезна лишь по отношению к решаемым задачам

6 Понятность – непонятность
зависит от того, насколько доступным для получателя информации языком она выражена

Ющук Е. Конкурентная разведка

Классификация источников информации

Первичные

сведения, полученные непосредственно от участников событий либо впервые ставшие доступные благодаря поиску

Вторичные

структурированная информация, собранная для определенных целей, отличных от целей, которые стоят перед аналитиком в данный момент

Внутренние

аналитик может получить данные из документов организации, к которым имеет доступ, или от ее сотрудников

Внешние

сведения принадлежат другим организациям либо общедоступны (СМИ, библиотеки)

Открытые

общедоступны, публичны, не требуют конфиденциальности

Закрытые

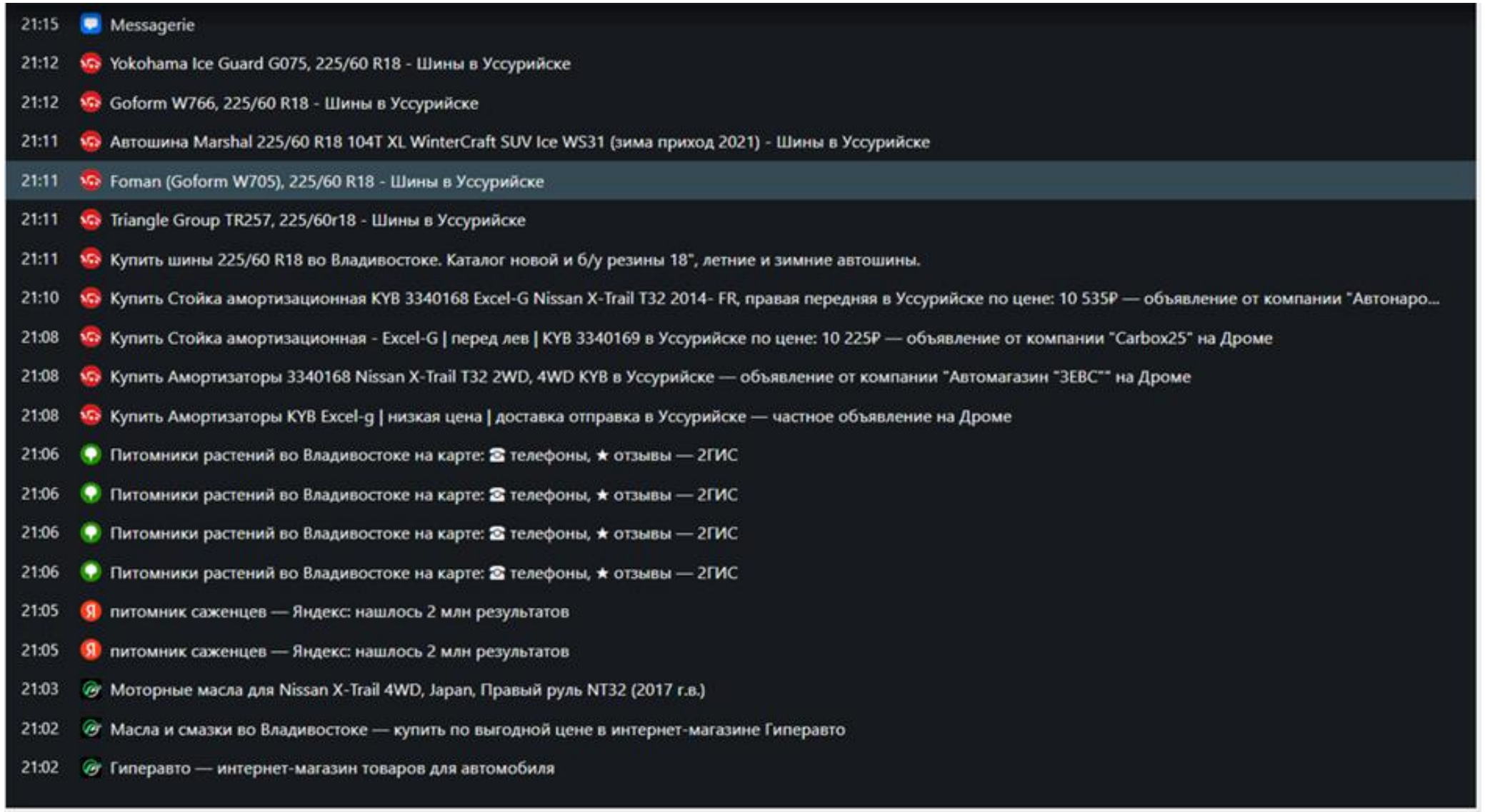
недоступны для всех желающих, использование часто незаконно

Плюсы и минусы OSINT

+ Минимальные риски
+ Экономическая эффективность
+ Удобство доступа
+ Правовые вопросы
+ Помощь правоохранительным и контрольным органам в финансовой сфере
+ Борьба с фейками в Интернете

- Огромный объем данных
- Надежность источников
- Трудоёмкость и жёсткие требования к квалификации аналитика, проводящего OSINT

Практический OSINT



Crowd-Source OSINT

« Худший в истории фоторобот» помог поймать преступника

За неделю до ареста в полицейские участки округа был разослан нелепый и убогий фоторобот, который стал предметом насмешек среди полицейских и местных жителей, которые растиражировали его в интернете.

Однако в итоге именно благодаря этому рисунку и был пойман злоумышленник Гленн Ранделс, которого обвиняют в ограблении с отягчающими обстоятельствами, непристойном обнажении, взломе жилища, хулиганстве и уклонении от ареста.

Босс итальянской мафии пойман благодаря Google

Босс итальянской мафии пойман благодаря Google

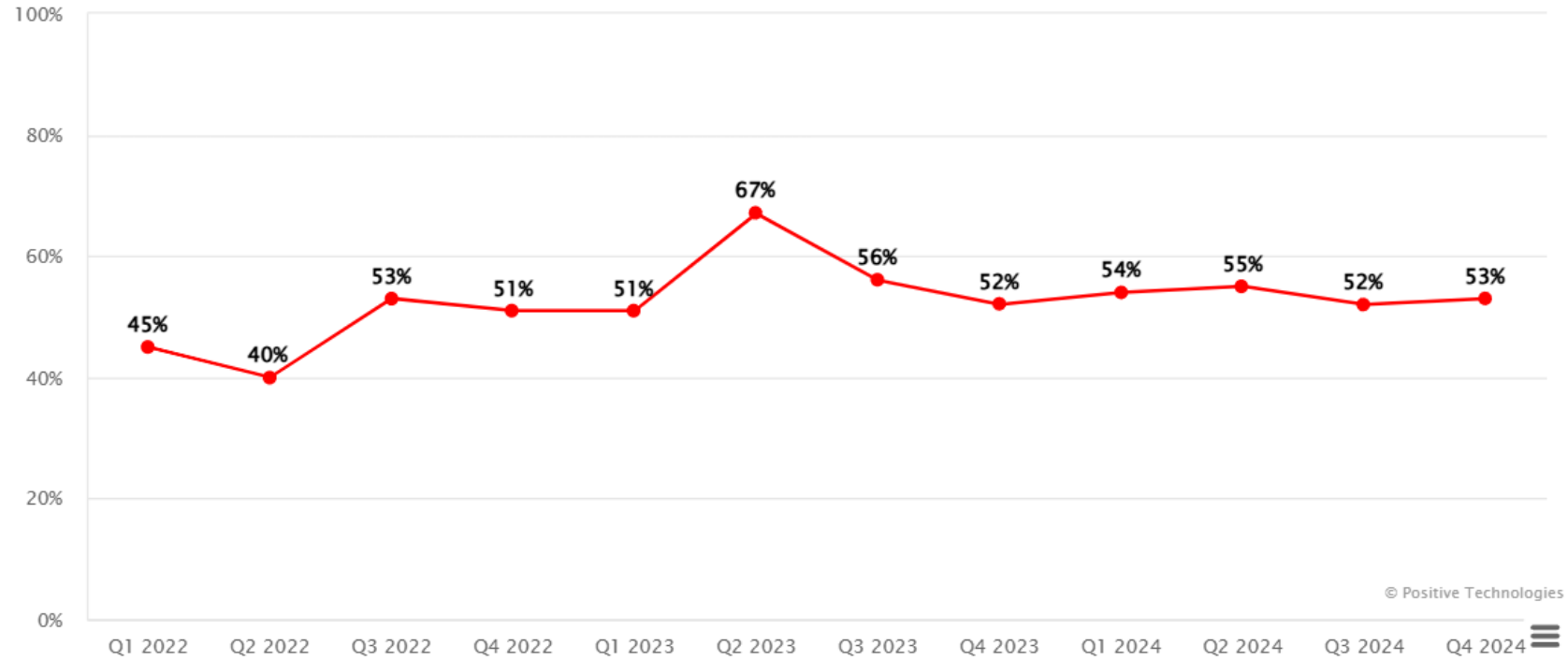
На одном из снимков, сделанных камерами сервиса Google Street View, полицейские опознали одного из самых разыскиваемых преступников – приговоренного к пожизненному заключению гангстера Джоаккино Гаммино. Вскоре мужчину задержали.

Выяснилось, что последние 20 лет Гаммино проживал в небольшом городе неподалеку от Мадрида, а местным жителям он был известен как Мануэль – владелец овощного магазина и шеф-повар ресторана.

Google и побег из тюрьмы

Статистика утечек данных в организациях

Рисунок 1. Динамика доли успешных атак на организации, закончившихся утечками данных



Сводная статистика по утечкам данных в странах

Продажа

28% ↘

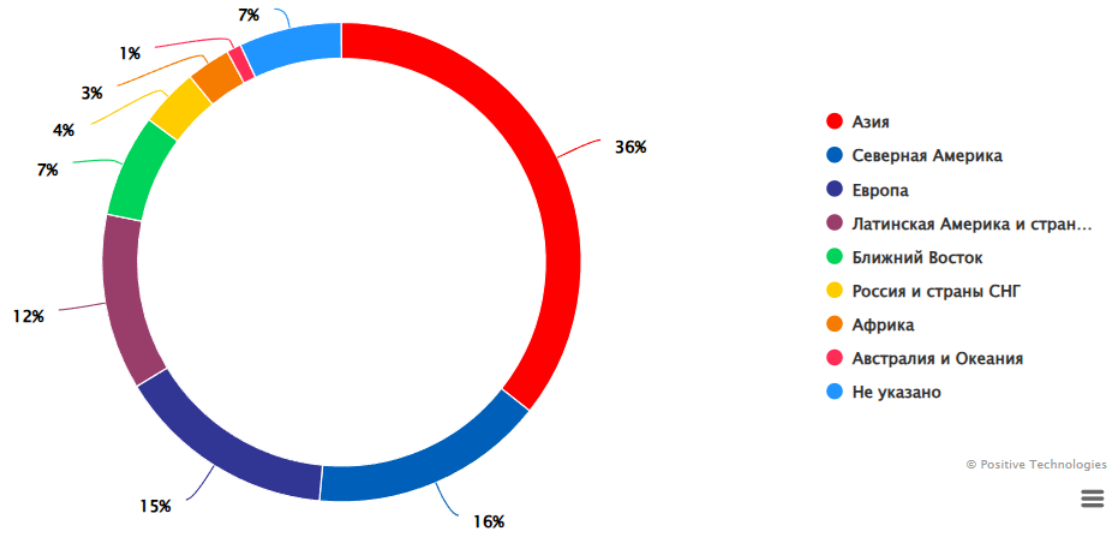
объявлений, связанных с утечками

Средняя* цена, указанная в объявлениях о продаже данных

Данные платежных карт	2500 $	Внутренние файлы	1500 $
Медицинские данные	2000 $	Учетные данные	1150 $
Исходный код	2000 $	Персональные данные	835 $

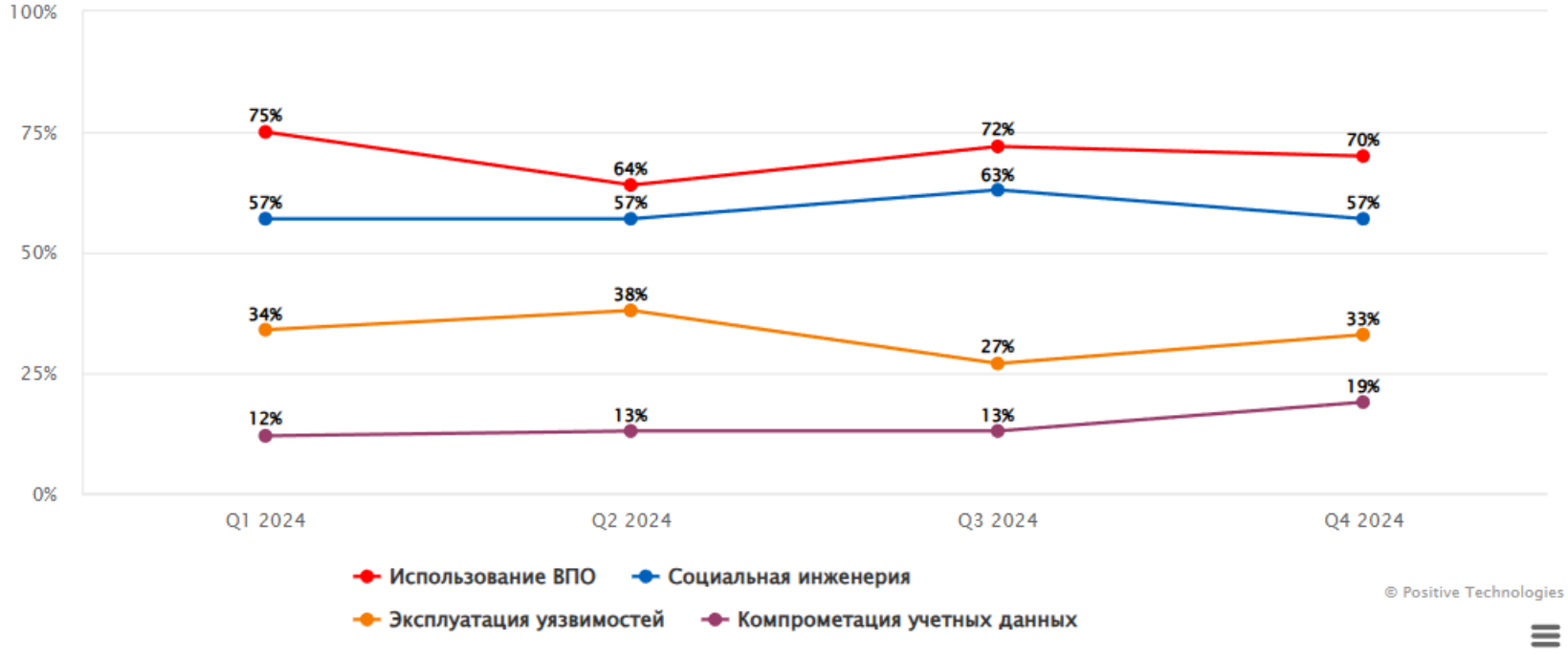
* В качестве среднего приведены медианные значения

Рисунок 23. Распределение объявлений по регионам



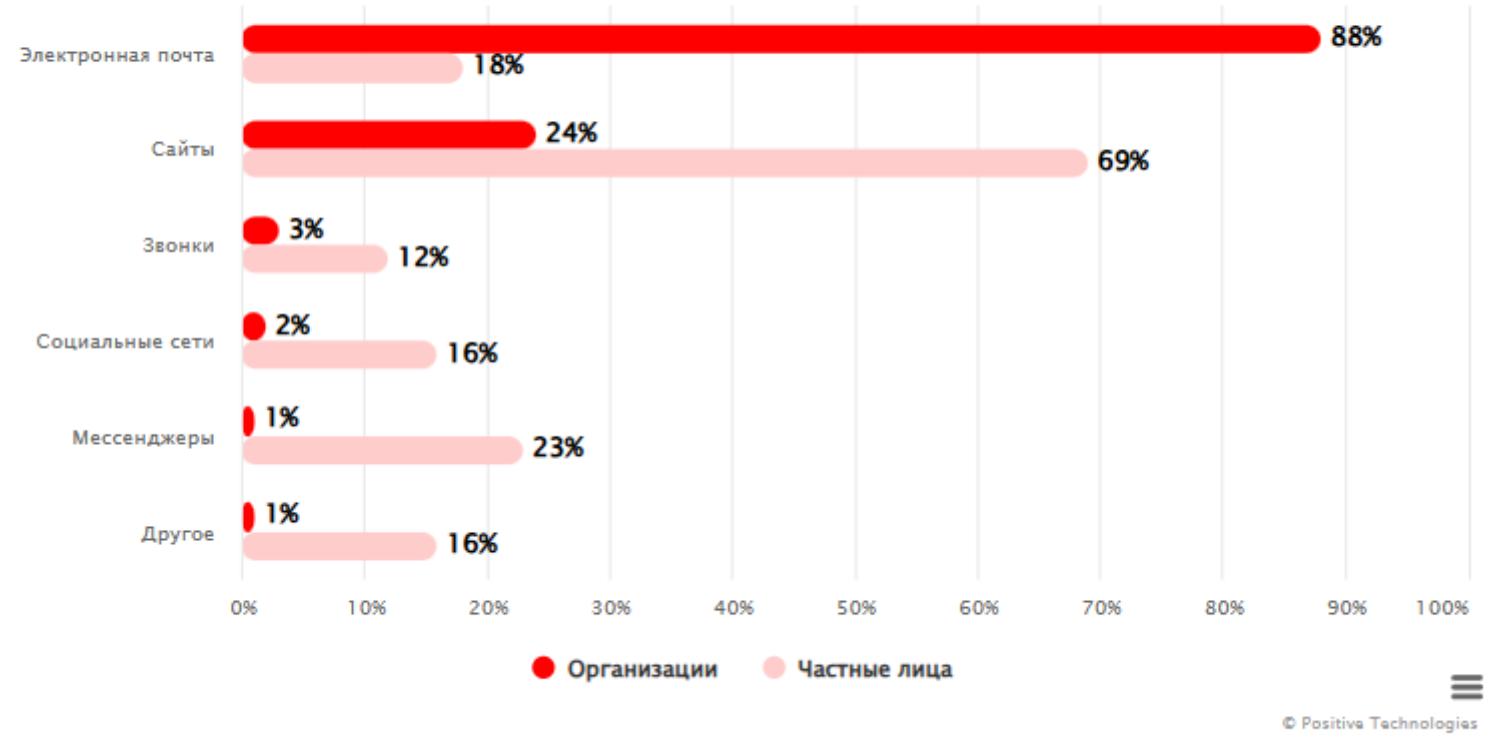
Методы организации утечек

Рисунок 39. Методы, использованные в успешных атаках на организации, последствием которых стали утечки

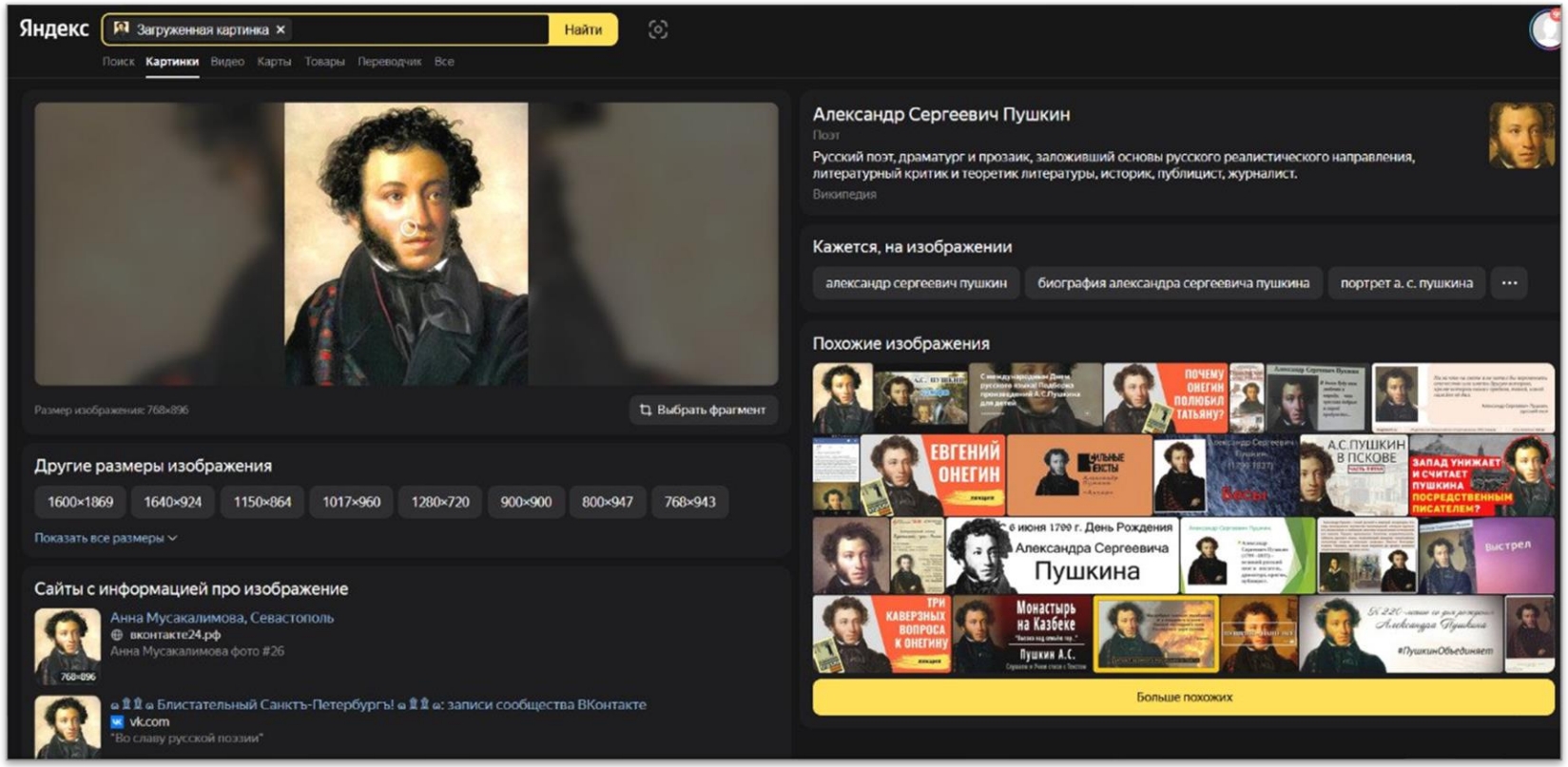


Каналы социальной инженерии

Рисунок 3. Каналы социальной инженерии (доля успешных атак, H1 2025)



Практический OSINT: Яндекс картинки



Яндекс картинки позволяют, используя фотографию объекта, найти ссылки или же подобные картинки. Это часто используется, когда нужно найти человека в другой соцсети.

Практический OSINT: Google Dorks

Операторы Google предоставляют сужать выдаваемую информацию поисковиком. Основные из них:

- site — искать по конкретному сайту;
- inurl — указать на то, что искомые слова должны быть частью адреса страницы / сайта;
- intitle — оператор поиска в заголовке самой страниц;
- filetype — поиск файлов конкретного типа по расширению.

Также при создании Дорка надо знать несколько важных операторов, которые задаются спецсимволами.

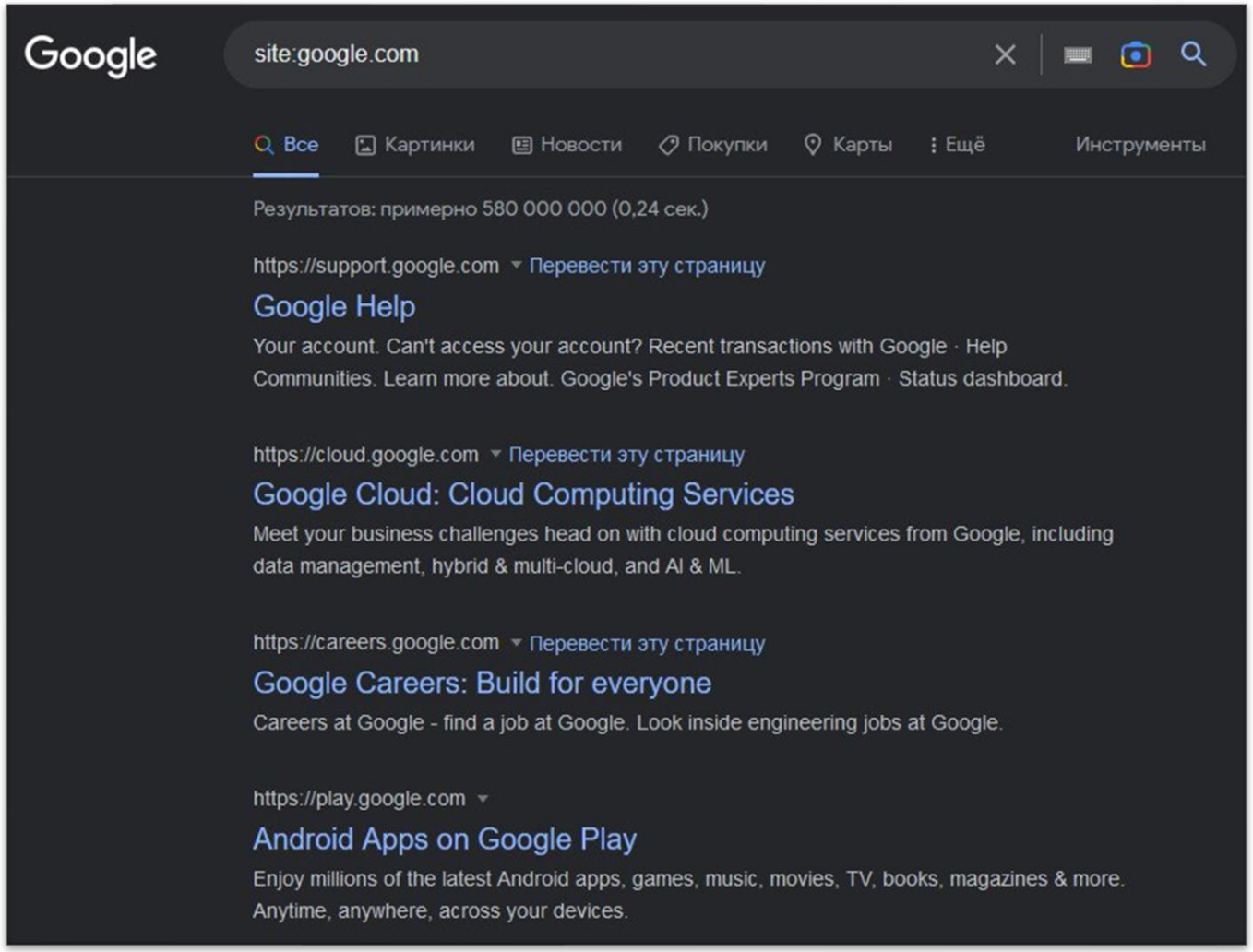
| — оператор OR он же вертикальный слеш (логическое или) указывает, что нужно отобразить результаты, содержащие хотя бы одно из слов, перечисленных в запросе.

«» — оператор кавычки указывает на поиск точного соответствия.

— — оператор минус используется для исключения из выдачи результатов с указанными после минуса словами.

* — оператор звездочка, или астериск используют в качестве маски и означает «что угодно».

Практический OSINT: Google Dorks

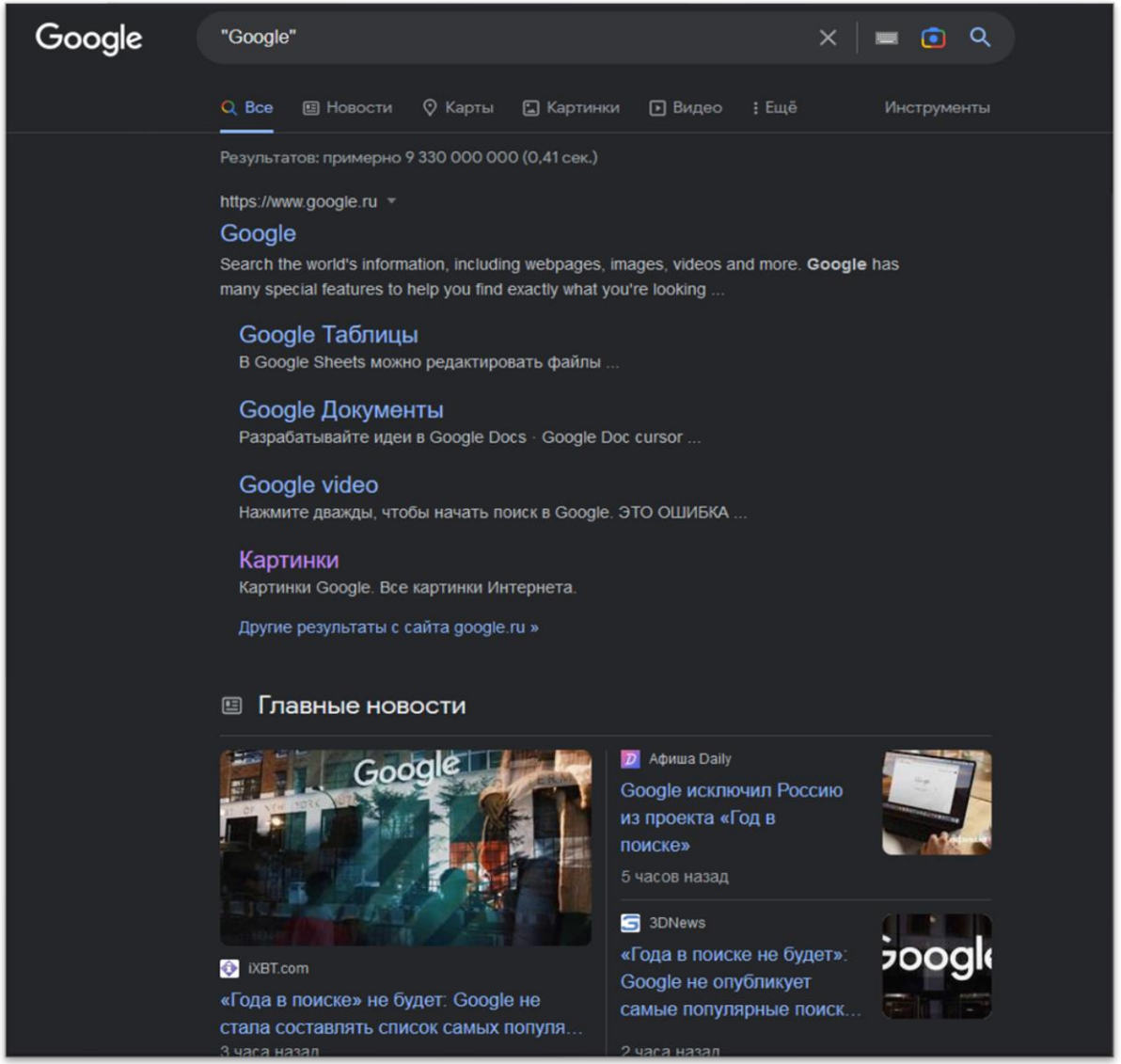


Google Dorks*

Поиск с помощью site

Как видим на скриншоте, поисковик выдал нам информацию, связанную с сайтом «google.com».

Практический OSINT: Google Dorks



Google Dorks

Поиск сайтов, где содержится определенное слово

На данный поисковый запрос, Google выдал нам сайты, где содержится слово «Google»

Данные запросы позволяют находить чувствительную информацию, как:
- Пароли
- Логи
- Открытые камеры
- И так далее…

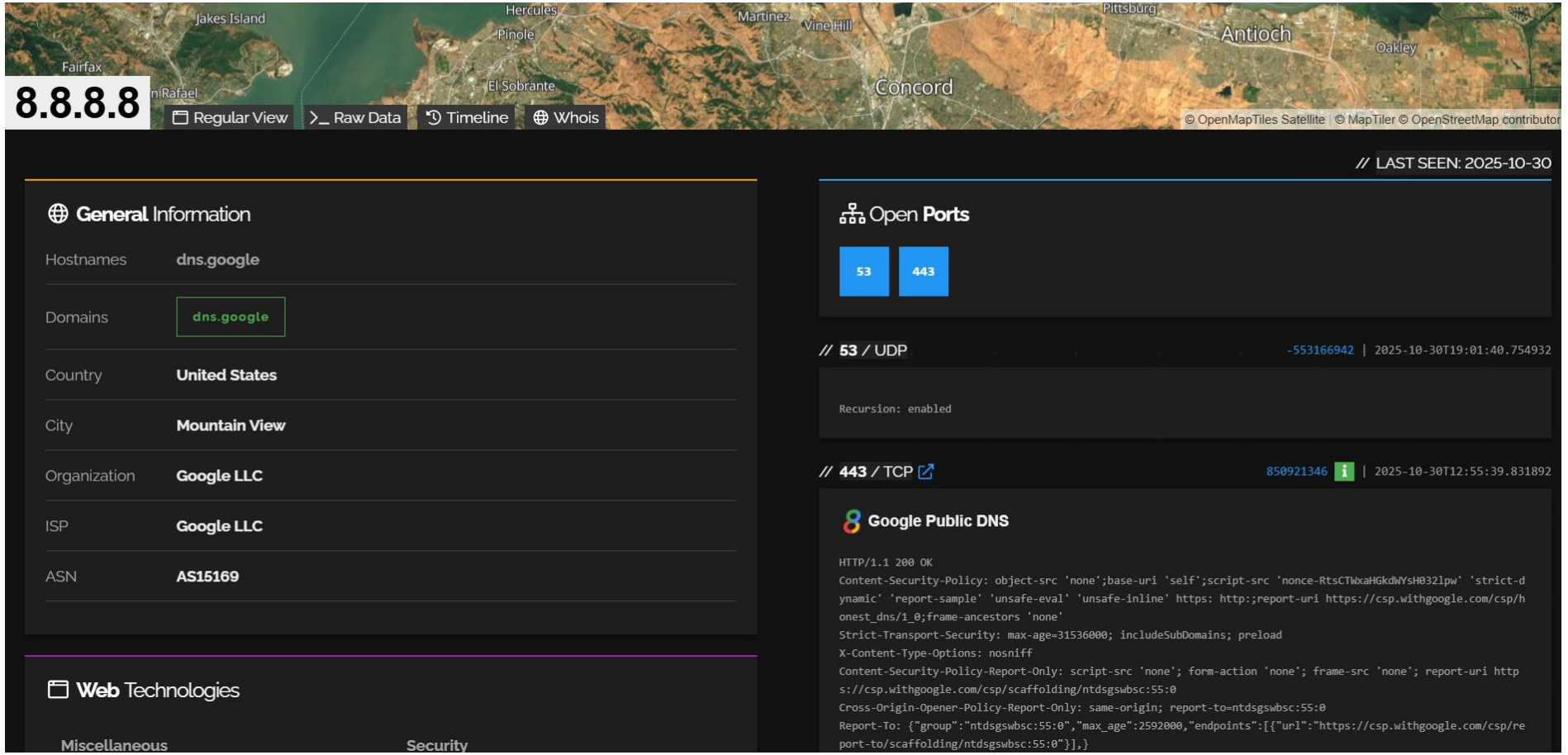
Практический OSINT: Shodan

Shodan — это поисковая система для поиска устройств, подключенных к Интернету, таких как серверы, веб-камеры и маршрутизаторы, используя различные фильтры. Она действует как поисковая система по сервисным баннерам — метаданным, которые серверы отправляют клиентам при подключении, и позволяет получать информацию об устройствах, находящихся в сети.

Что может собирать Shodan:

- Название и тип устройства
- Имя пользователя и пароли по умолчанию
- Географическое положение

Практический OSINT: Shodan



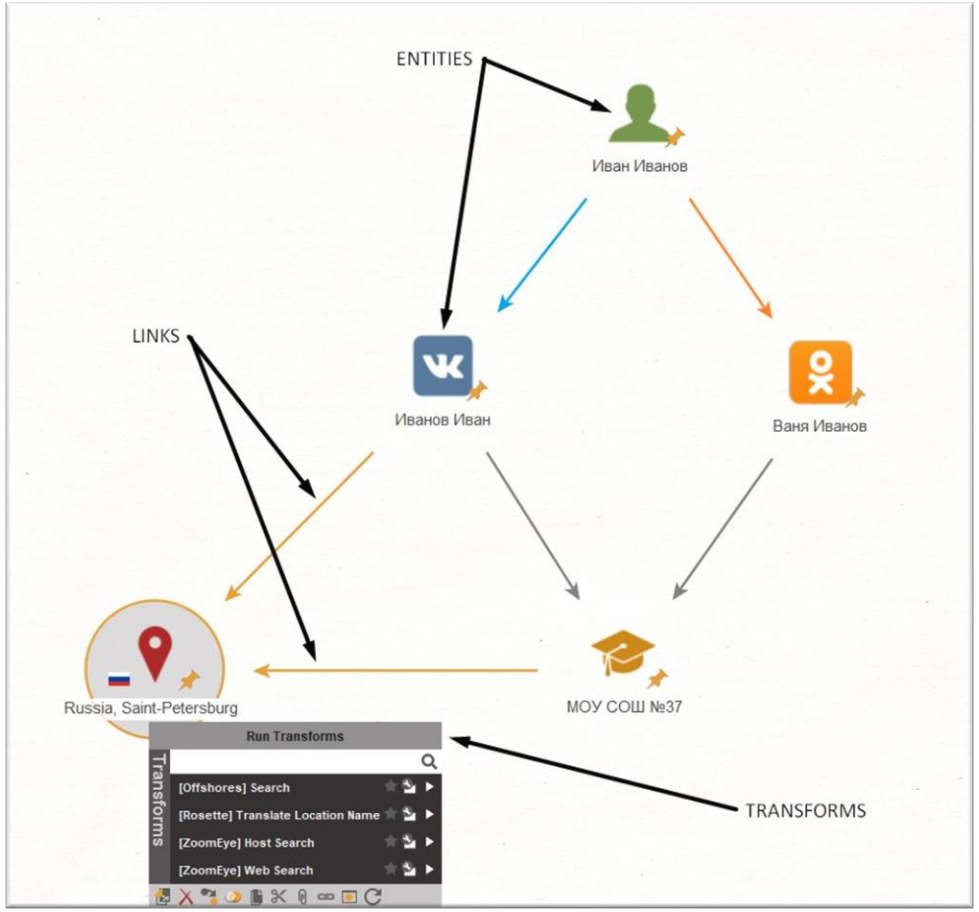
По IP адресу 8.8.8.8 (который принадлежит Google) мы нашли, что айпи адрес действительно принадлежит Google. Описаны открытые порты, информация, получаемая с них и геолокация.

Практический OSINT: Maltego

Maltego позволяет искать информацию и формировать граф зависимостей.

Данное ПО можно представить как доску для детективов, где наглядно понятно: что из чего следует. Данный инструмент облегчает строить связи между объектами исследований.

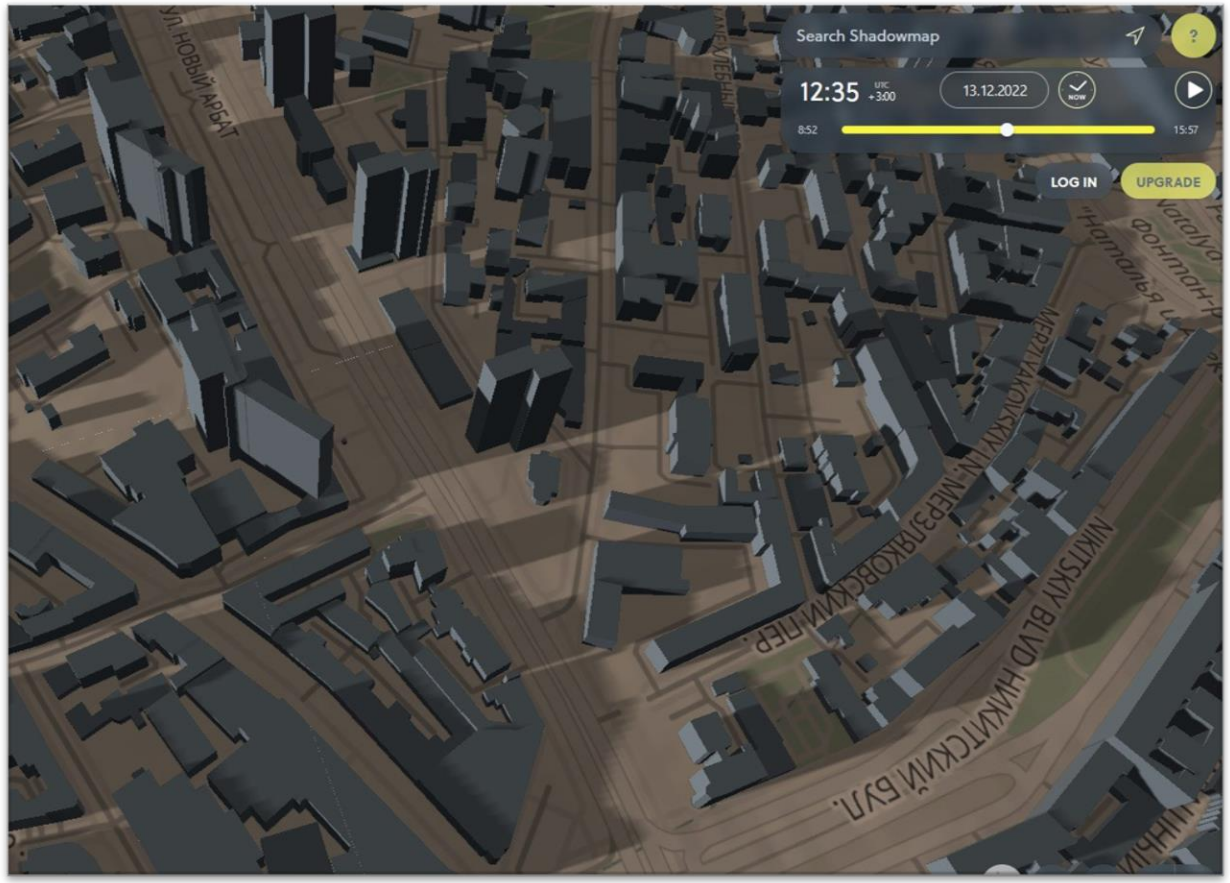
Здесь построена связь информации об вымышленном персонаже Иване Иванове.



Практический OSINT: ShadowMap

Данный инструмент помогает определить положение солнца в любой момент времени.

Используя ShadowMap, разведчик способен по углу падения солнечных лучей определить точное место съёмки (при условии того, что примерный радиус геопозоции мы знаем)



Выявление и отслеживание киберпреступников

В случае с Breach Forums исследователи могли отслеживать деятельность ключевых фигур, таких как "pompompurin" и "IntelBroker", используя комбинацию технической и социальной разведки.

Использовались методы форензики, отслеживания паттернов в общении и анализа взломанных систем.

OSIVE (Open Source Intelligence Visualization Engine) помогает следователям агрегировать и визуализировать утечки данных, такие как адреса электронной почты, пароли и другую личную информацию, найденную на форумах в темной паутине или на подпольных рынках.

С помощью этих инструментов аналитики, занимающиеся разведкой угроз, могут выстраивать взаимосвязи, отслеживать цифровые личности и соотносить данные по нескольким утечкам, чтобы лучше понять поведение и сети субъектов угроз.

Поиск киберпреступника

IntelX позволял пользователям исследовать прошлые утечки данных.

Это вызывало возмущение среди участников подпольных форумов.

В ответ на это члены форумов организовали доксинг против Кляйснера, распространяя его личную информацию, такую как адрес и телефонные номера, с целью запугивания и дискредитации.

ссылка на статью с разбором отслеживания по шагам

1. Корреляция данных: Методы сопоставления собранных данных для выявления закономерностей и связей между участниками и событиями.

2. Анализ настроений: Использование технологий обработки естественного языка (NLP) для оценки общественных настроений и реакции на события.

3. Анализ сетей: Составление карт взаимосвязей участников на основе данных для выявления криминальных сетей.

90 процентов разведданных приходит из открытых источников и только 10 — за счёт работы агентуры

— генерал-лейтенант Самуэль Уилсон, руководитель Разведывательного управления Министерства обороны США