OSINT

Разведка по открытым источникам

Разведка по открытым источникам

Разве́дка по откры́тым исто́чникам (англ. **Open source intelligence, OSINT) —** разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ и систематизацию.

*wikipedia

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.

OSINT - это легально

Сбор данных из открытых источников

Что это такое?

Легальный способ получения информации из публичных источников для личных или профессиональных целей

Где искать данные?

Официальные сайты, отраслевые порталы, социальные медиа, форумы и другие открытые источники

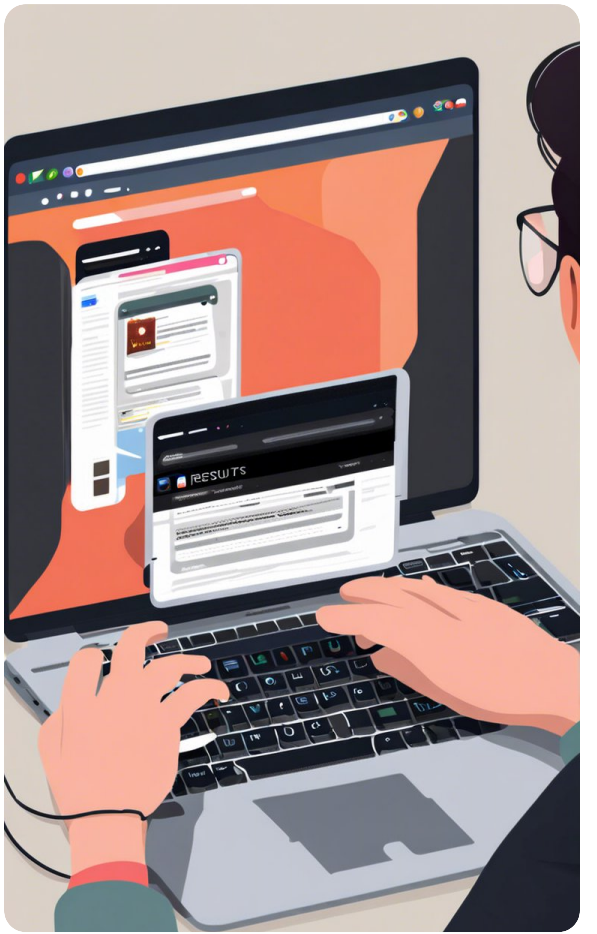
Как использовать данные?

OSINT для расследования внутренних инцидентов

Поиск в Интернете

Эффективные методы сбора OSINT-информации

1. **Ручной поиск в Google, Yandex**
2. **Использование специализированных сервисов**
3. **Анализ профилей в соцсетях**
4. **Мониторинг форумов и чатов**



Поиск информации

- поиска по имени и по нику (Maryam,Snoop,Alfred)
- поиске по изображению (search4face.com)
- поиск по местности (2gis,DualMaps,demo.f4map)
- поиск по Email (haveibeenpwned.com, Ghunt)
- поиск по номеру телефона (PhoneInfoga)

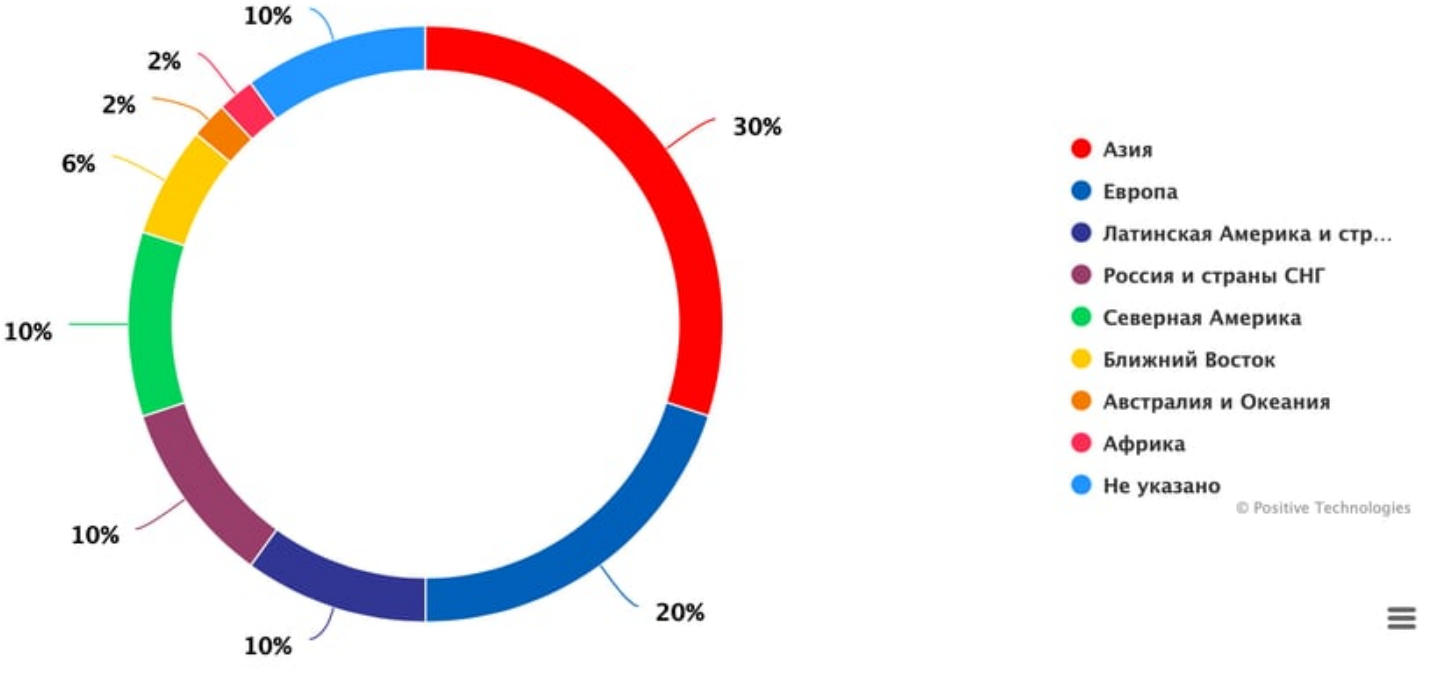
Проведите свое расследование

Codeby.games

Osint Tasks Bot

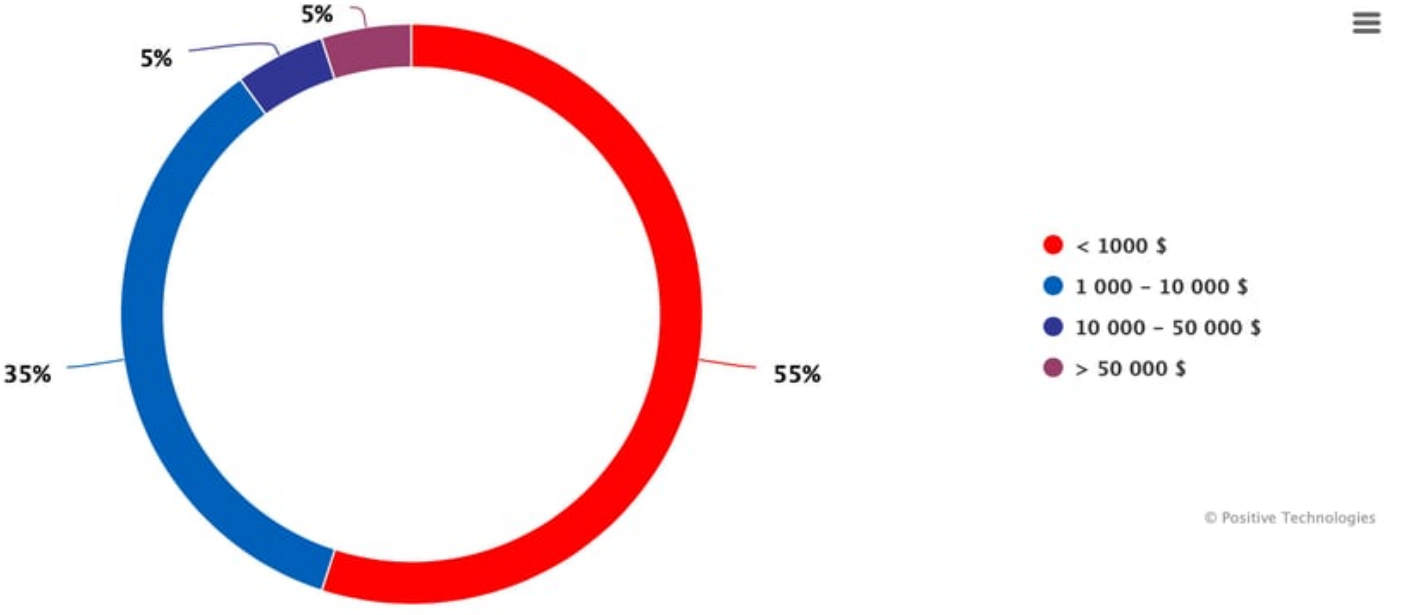
Теневой рынок данных — общая статистика

Рисунок 1. Распределение объявлений по регионам



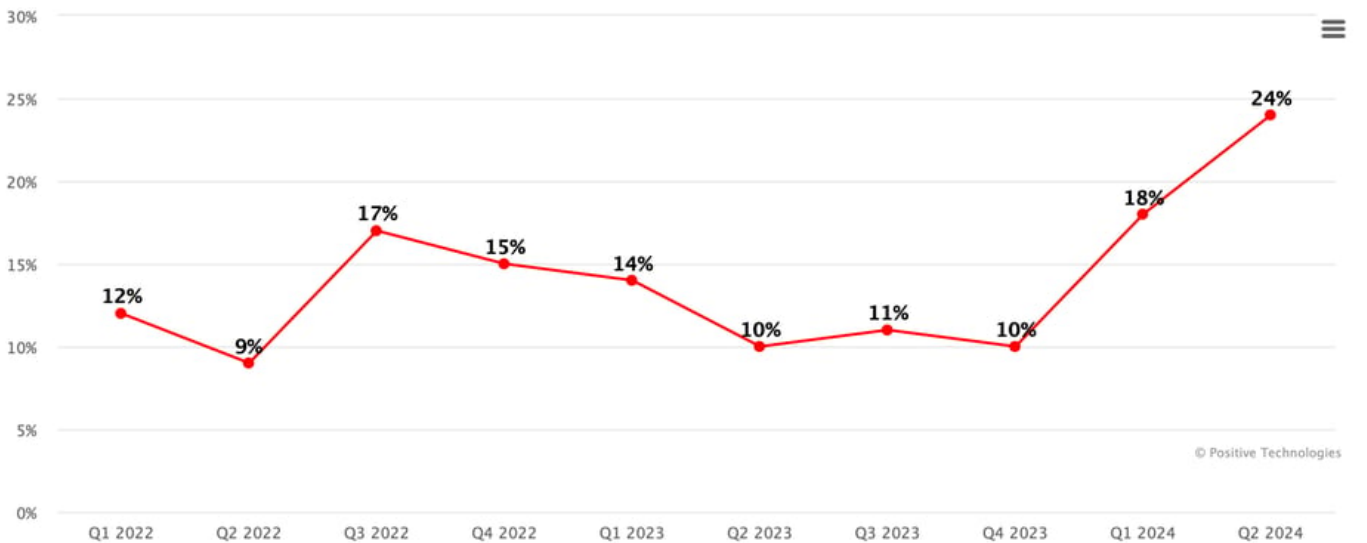
Теневой рынок данных — цена

Рисунок 2. Диапазон цен объявлений на теневом рынке о продаже баз данных

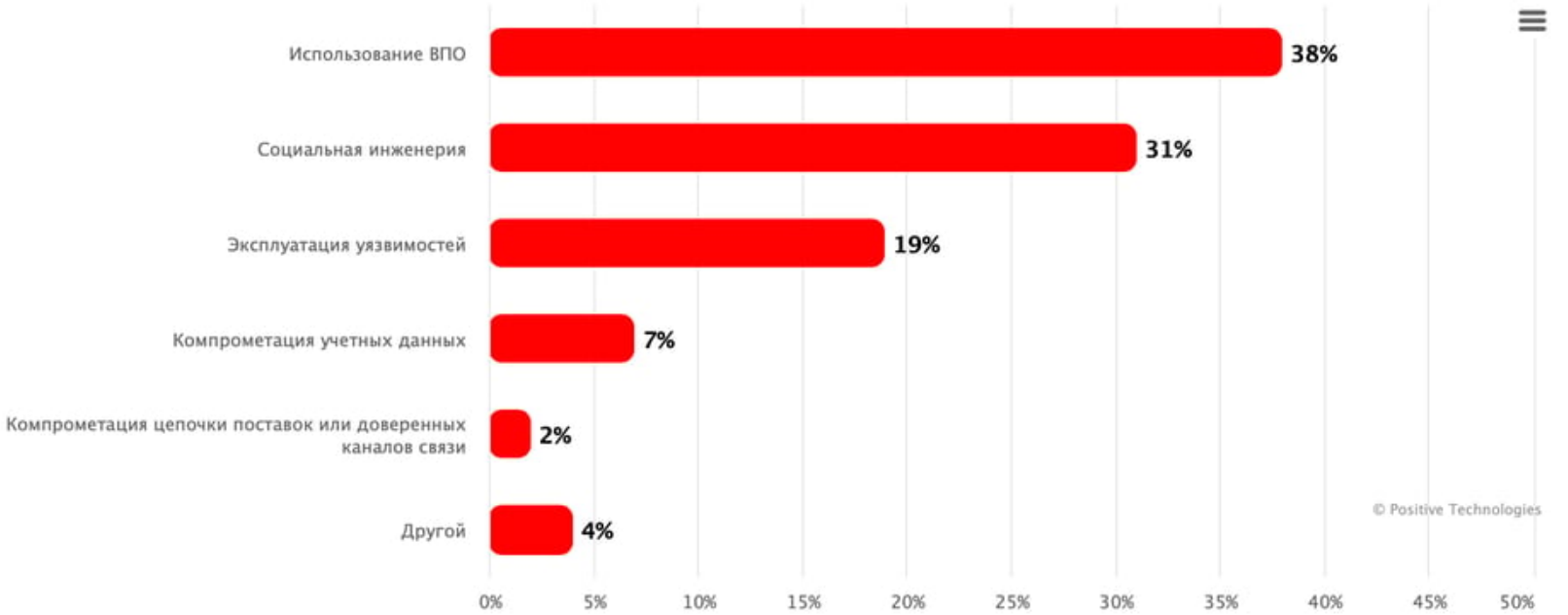


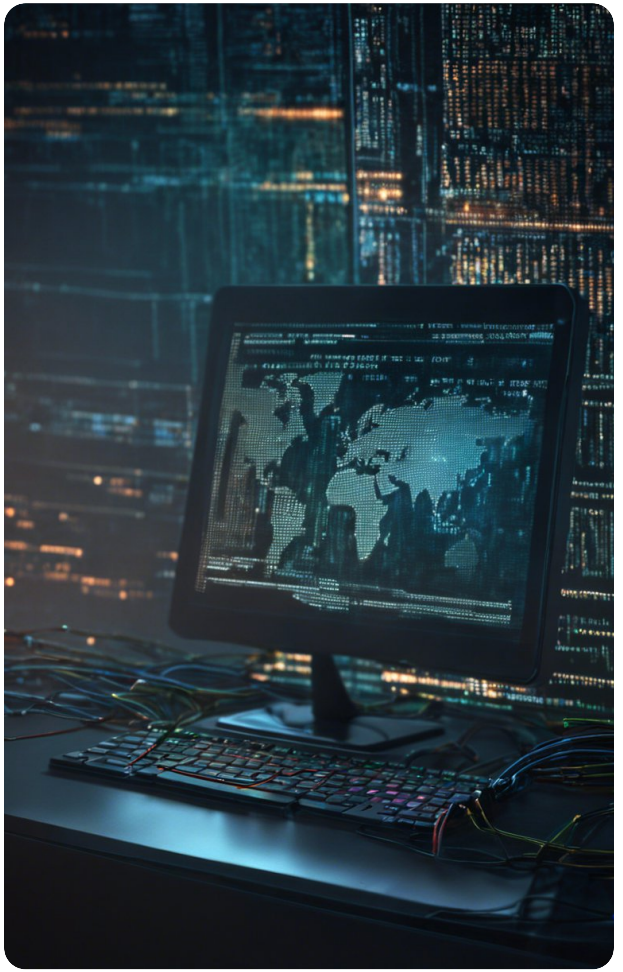
Активный рост числа утечек учетных

Рисунок 11. Динамика утечек учетных данных у организаций (2022 год – первое полугодие 2024 года)



Методы успешных атак





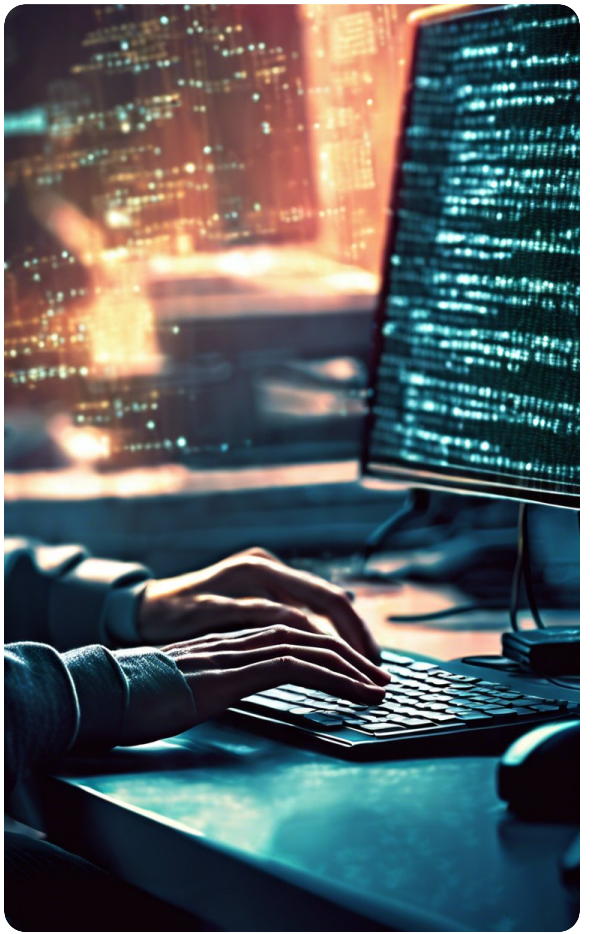
OSINT — инструменты для выявления лиц, скрывающихся в сети

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

Выявление и отслеживание киберпреступников

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.



Разоблачение Pompompurin

Сопоставление активности пользователей с утечками учетных данных и метаданными с архива Breach Forums позволило следователям установить связи, ведущие к Фицпатрику.

```
PE[CC3A6F123D8BA8ACF36E83F46EBF2BE9] [2023-01-02T18_03_35.9379073].zip.zip
Url: https://signup.lan.leagueoflegends.com/es/signup/index
Username: Pompompurin
Password: marshalteamo666
Insertion Timestamp: 2023-10-09 12:00:00+02:00

PE[CC3A6F123D8BA8ACF36E83F46EBF2BE9] [2023-01-02T18_03_35.9379073].zip.zip
Url: https://signup.las.leagueoflegends.com/es/signup/index
Username: Pompompurin
Password: marshalteamo666
Insertion Timestamp: 2023-10-09 12:00:00+02:00

Url: https://signup.las.leagueoflegends.com/es/signup/index
Username: Pompompurin
Password: lucifer2005
Insertion Timestamp: 2023-08-11 17:01:20.227305+02:00

sources: ['gPotato.com']
username: pompompurin
password: badboyssky
lastbreach: 2006-11

sources: ['Stealer Logs']
username: pompompurin
password: marshalteamo666
lastbreach:
```

IntelX

- 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.

Поиск киберпрестпупника

методы анализа

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.

Шаг 1: Проверка личности и биографии

Основные данные:

•Имя: Конор Брайан Фицпатрик

•Дата рождения: 26 сентября 2002 г.

•SSN(номер соц. страхования): 081-92-4399

•Адрес: 531 Union Ave, Peekskill, NY 10566

•Телефоны: +1 914 642 3144, +1 914 402 5399, +1 9146999668

- Поиск по публичным документам: Для проверки личности и связанных данных используются публичные поисковые системы, такие как Whitepages и Pipl. Эти сервисы помогают проверить, совпадают ли данные, такие как адрес, с реальной информацией.
- Подтверждение адреса: Используем гугл карты чтобы подтвердить физический адрес (537 Юнион-авеню, Пикскилл, Нью-Йорк). "Просмотр улиц" и информация об адресе поможет идентифицировать визуально.
- Пробив номера телефона: Нужно использовать сервисы по поиску номера телефона как TrueCaller, NumLookup или SpyDialer чтобы определить что номера действительны и зарегестрированы на одного человека. Также необходимо проверить операторов типа Verizon Wireless и Cablevision Lightpath.

Шаг 2: Анализ социальных сетей и онлайн-следа

Основные данные:

•Электронная почта: pom@pompur.in

•Twitter: https://twitter.com/xml

•Telegram: https://t.me/paste

- Отслеживание электронной почты: проверка, связана ли электронная почта с утечками данных. Можно также определить, на каких сервисах зарегистрирована эта электронная почта.
- Анализ Твиттера: Проведите анализ ручек Twitter с помощью таких инструментов, как Twitonomy или TweetBeaver. Это поможет выявить шаблоны твитов, связи, подписчиков и любую историю твитов, которая может свидетельствовать о личной или незаконной деятельности.
- Скраппинг групп в Telegram: Используйте Telegago или Telegram OSINT Tool для изучения активности пользователя в Telegram. Ищите членство в группах, общие файлы или возможные ссылки на форумы темной паутины или преступные сообщества.

Шаг 3: Родственники и семейные связи

Основные данные:

•Мать: Мэри МакКарра Фицпатрик (год рожд.: 1967)

•Отец: Марк Э. Фицпатрик (год рождения: 1961)

•Младший брат: Брендан Фицпатрик

•Брат с тяжёлой формой аутизма: Эйден Фицпатрик

- Инструменты семейного поиска: Используйте генеалогические сайты, такие как FamilyTreeNow или Ancestry.com, чтобы проследить историю семьи и подтвердить указанные связи. Это поможет подтвердить личные связи и может выявить дополнительных родственников.
- Поиск в социальных сетях: Найдите членов семьи в Facebook, LinkedIn или Instagram, используя их полные имена и даты рождения. Это поможет вам составить схему социальных связей семьи, её привычек и любых видимых связей с деятельностью цели.
- Проверка публичных записей: Используйте такие сервисы, как MyHeritage или PeopleFinders, чтобы найти адреса, номера телефонов или любые судимости, связанные с членами семьи.

Шаг 4: Юридические документы и судебные записи

Основные данные:

•Имя: Конор Брайан Фицпатрик

•Арест ФБР: Связан с компьютерными преступлениями, вероятно, с работой Breach Forums.

- Поиск судебных документов: Выполните поиск открытых судебных документов с помощью CourtListener, PACER или Justia Dockets. Эти платформы предоставляют доступ к судебным документам, обвинительным заключениям и сопутствующим материалам дела. Пример: Поиск записей, связанных с арестом ФБР, может выявить точные обвинения, судебные разбирательства и приговор.
- Сообщения СМИ: Используйте такие инструменты, как Google News и Factiva, чтобы собрать сообщения СМИ, связанные с арестом Конора Брайана Фицпатрика. Статьи из авторитетных источников, таких как Krebs on Security или Bloomberg (как указано выше), предлагают подробную информацию о преступной деятельности и расследованиях.

Шаг 5: Поиск в темной паутине и на подземных форумах

Основные данные:

•Псевдонимы/Ник: Pompurin

•Присутствие в сети: Администратор Breach Forums, Skidbin и других тёмных веб-сообществ.

- Мониторинг тёмной паутины: Используйте такие инструменты OSINT, как DarkOwl, IntelX или RecordedFuture, для мониторинга форумов и торговых площадок тёмной паутины на предмет упоминаний "Pompompurin" или других связанных с ним псевдонимов. Эти платформы часто индексируют активность в тёмной паутине и могут предоставить массу информации.
- Анализ форума: Исследуйте Breach Forums и все оставшиеся архивы Skidbin, чтобы найти сообщения, сделанные Pompompurin. Используйте методы скраппинга форумов или пользовательские запросы для извлечения данных, связанных с незаконной деятельностью. Обратите внимание на подпольные связи и потенциальные связи с другими киберпреступниками.

Шаг 6: Поиск утечки данных и финансовая информация

Основные данные:

•SSN(номер соц. страхования): 081-92-4399

•Электронная почта и другие аккаунты

- HaveIBeenPwned: Используйте этот инструмент, чтобы узнать, не были ли SSN, электронная почта или другие связанные с ними учетные записи утечкой данных в прошлом. Это поможет определить, не скомпрометированы ли данные этого человека.
- Финансовое отслеживание: Вы можете воспользоваться такими сервисами, как BeenVerified или LexisNexis, чтобы провести проверку биографии, включающую финансовую историю, записи о возможных банкротствах и владении активами, связанными с объектом поиска.

Запретить **OSINT** невозможно.