



OSINT в расследовании киберинцидентов v 0.0.4

ДОКЛАДЧИК: @soxoj

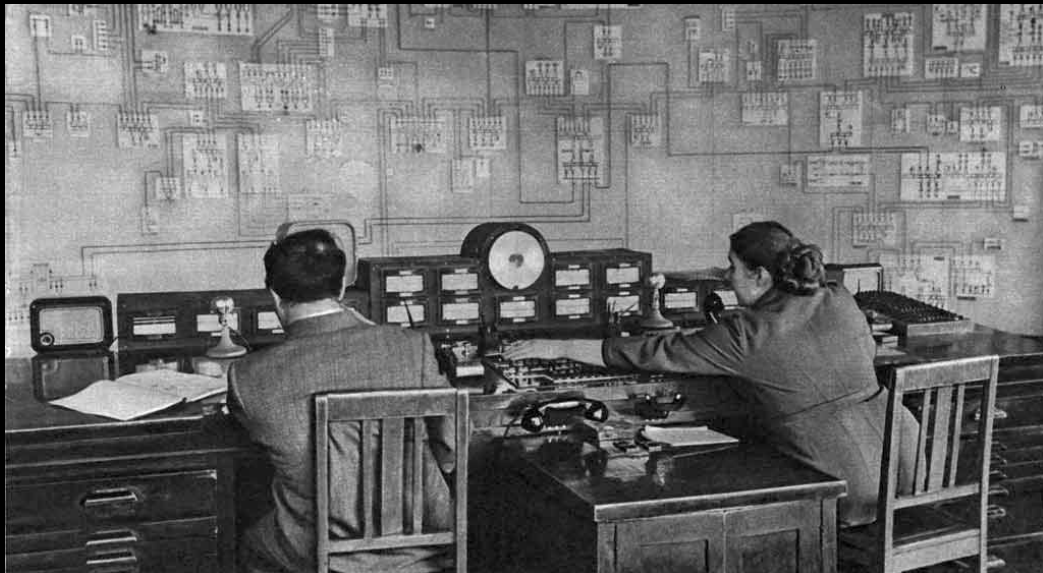


Open-source intelligence

Разведка на основе открытых источников

90 процентов разведданных приходит из открытых источников [1]

Пример: ЦРУ составило схему электроснабжения советской ядерной программы по фотографии из журнала “Огонёк” [2]



[1] <https://vpk-news.ru/articles/7324>

[2] <https://vakhnenko.livejournal.com/235426.html>



- Внешний нарушитель
 - DoS
 - Фишинг
 - Малварь
- Внутренний нарушитель
 - Утечки данных
 - Атаки изнутри

Основная цель -- **определение субъекта-нарушителя**

Примеры: Конкурентная разведка на PHDays [1], CTF HackIt-2017 [2]

[1] <https://habr.com/ru/company/pt/blog/413203/>

[2] <https://habr.com/ru/post/338078/>



- 01. Company real name: 191
- 02. IDOR specialist username: 166
- 15. Petr's primary e-mail. We know he's looking for a job: 126
- 03. IDOR specialist location (format location1, location2): 88
- 18. Donation wallet number: 76
- 04. IDOR specialist work e-mail: 74
- 16. Petr's secondary e-mail: 71
- 06. Secret employee mobile phone: 50
- 10. Nightly programmer private username: 36
- 19. Software which was downloaded from IP 77.71.34.171: 32
- 17. Petr's password: 19
- 08. Secret employee birthday (format dd.mm.yyyy): 34
- 11. What the flag?: 11
- 13. IP used in PoC script: 10
- 12. Second employee IM username/ID: 7
- 14. Alexander's real lastname: 4
- 07. Secret employee username: 3
- 05. IDOR specialist personal e-mail: 1
- 09. Secret employee university: 0

Protected: My secret page

May 10, 2019

This content is password protected. To view it please enter your password below:

Password:

Enter

May 10, 2019 Uncategorized


Published by Matumbo Harris Nightly Programmer

[View more posts](#)

PHDays 9 CI: КАК ЭТО БЫЛО

PHDays 9
OSINT в расследовании киберинцидентов
phdays.com / dc7495.org







 Покупки по категориям ▾


Найдите любые товары



Все категории ▾

Найти

Расширенный


   




a02f954   Больше не является зарегистрированным пользователем

Товары в продаже

Hi! My name is A. Bassur. At the moment, all goods are sent from Phoenix, Arizona


05.2019 |  Россия



Abdul Bassur
Deputy CEO – Self-XSS security
Phoenix, Arizona

Отправить сообщение

...




Deputy CEO
IDOR Security
май 2019 · 1 мес.
contact: p@nfsg64ttmvrk4tjor4q.club

PHDays 9 CI: КАК ЭТО БЫЛО

PHDays 9
OSINT в расследовании киберинцидентов
phdays.com / dc7495.org





Petr Ananov
Безопасность, IDOR, IDOR Security,
IDORSecurity
Старший (Senior)
[nfsg64ttmvrk4tjor4q.club](#)

Ищу работу

[Запрос отправлен](#) [К диалогу](#) [...](#)

Друзья 0

Рекомендательные письма 0

Активность
Регистрация: 17.05.2019
Последний визит: 4 дня назад

Местоположение
Россия, Москва

Возраст и стаж
Возраст: 30 лет
Опыт работы: 2 месяца

Контакты
Почта: ananevpetr1988@mail.ru
[nfsg64ttmvrk4tjor4q.club/](#)


Обо мне

IDOR Security CTO.


Профессиональные навыки

Информационная безопасность • Администрирование Windows

Опыт работы

 **IDOR Security**
CTO
Апрель 2019 — По насто
IDOR Expert
Clickjacking boob

Высшее образование

 **Томский технику**
ОГБПОУ «Томский техн
Томск • 18 выпускников
Май 2019—По настояще

[pwned?](#)

Oh no — pwned!
Pwned on 5 breached sites and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security [Start using 1Password.com](#)

**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.

**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.

**Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

[f](#) [t](#) [b](#) [p](#) [Donate](#)


Breaches you were pwned in
A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

**000webhost:** In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.
Compromised data: Email addresses, IP addresses, Names, Passwords

Проверьте почту

[ananevpetr1988@mail.ru](#) [Изменить](#)

В течение 15 минут вы получите письмо на почту **adm**@rus-samp.ru**. Когда письмо придёт, перейдите по ссылке.



[получается ВОССТАНОВИТЬ](#)

```
$ grep admin@rus-samp.ru  
000webhost_13mil_plain_Oct_2015.txt  
Mark:admin@rus-samp.ru:83.239.102.7:darkma95
```

PHDays 9 CI: СХЕМА РЕШЕНИЯ

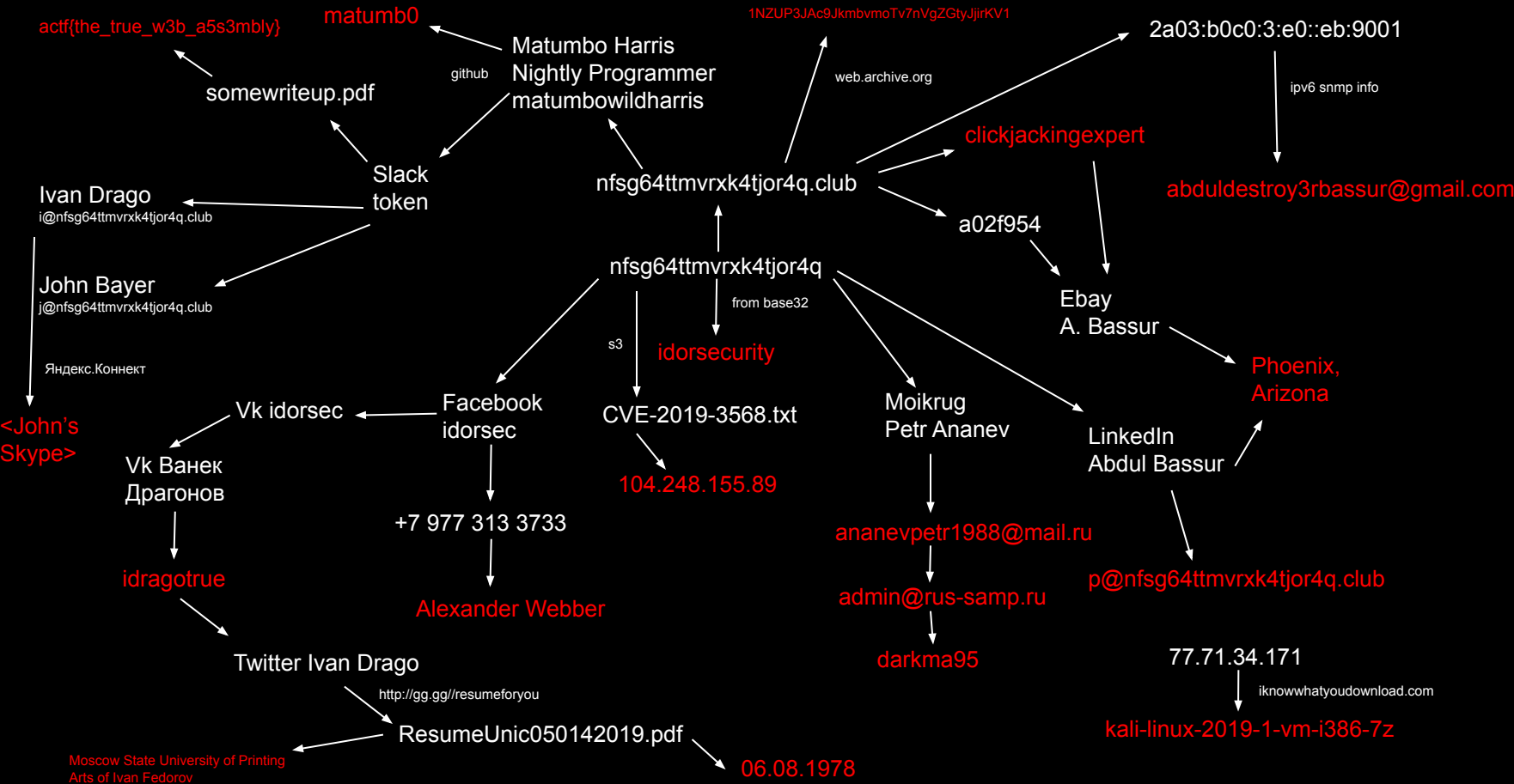
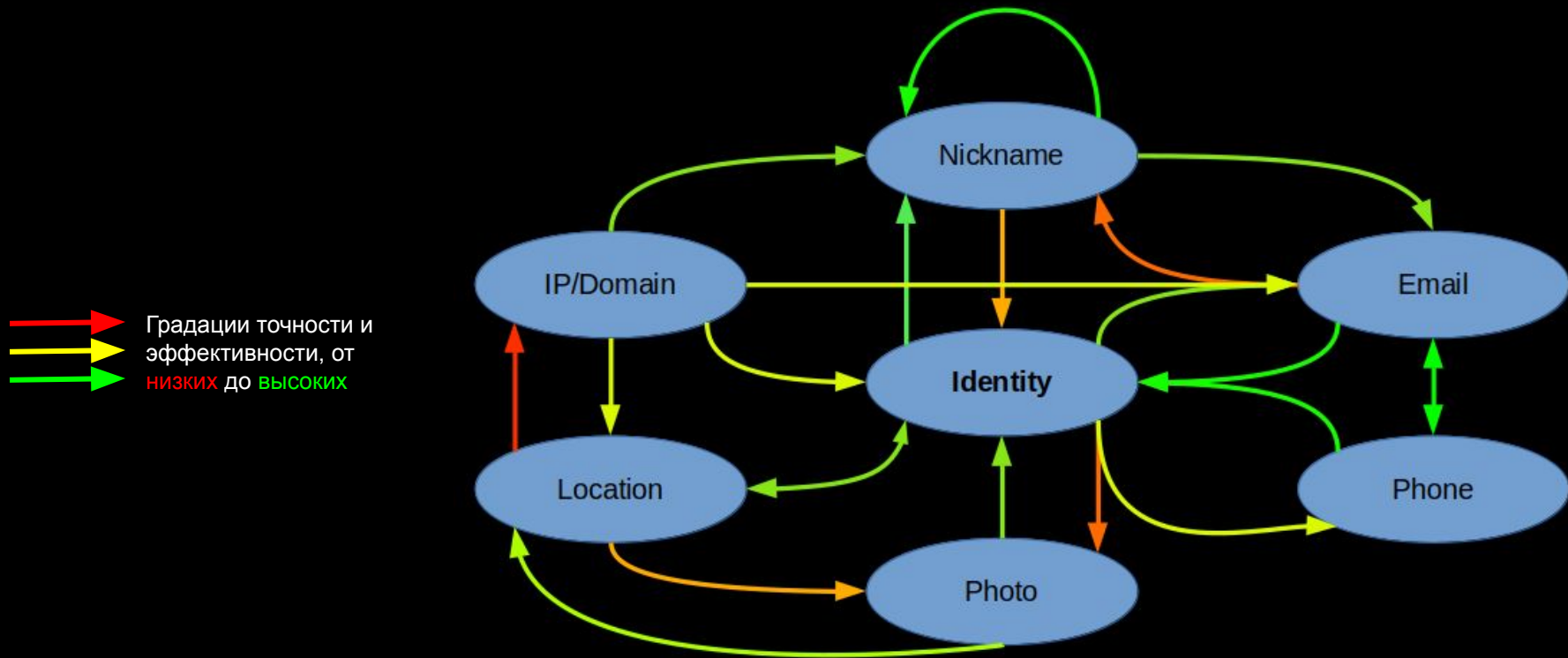


СХЕМА ПОИСКА НАРУШИТЕЛЯ



БАЗОВЫЕ ПРИНЦИПЫ ПОИСКА

PHDays 9
OSINT в расследовании киберинцидентов
phdays.com / dc7495.org



Мало сделать запрос в Google, надо уметь им пользоваться.

- Составить план
- Уточнять запросы
- Отсекать лишнее
- Обновлять цель
- Понимать, где и что искать

Fravia - реверс-инженер и искатель [1]



[1] https://t.me/netstalking_overground/78



МАМОНТ

☐ - Искать в найденном ☐ Поиск в Интернете ☒ Поиск файлов

Всего файлов найдено: **20**

-15 -14 -13 -12 -11 -10 -09 -08 -07 -06 -05 -04 -03 -02 -01 страница **01** из **01**
+01 +02 +03 +04 +05 +06 +07 +08 +09 +10 +11 +12 +13 +14 +15 <- назад | следующая ->

1. [ftp://\[redacted\]/time500/infa kolya/rabstol/СИБГТУ/5 сессия 2014/тпкмашов/Шмелев Дмитрий/Паспорт \(2\).jpg](ftp://[redacted]/time500/infa kolya/rabstol/СИБГТУ/5 сессия 2014/тпкмашов/Шмелев Дмитрий/Паспорт (2).jpg)

регион	проверен	изменен	размер файла
Россия	9 января 2016	21 июля 2014	290.12Kb [297 085 байт]
[похожие файлы] [найти файлы такого же размера] [искать только на этом сервере]			

2. [ftp://\[redacted\]/time500/infa kolya/rabstol/СИБГТУ/5 сессия 2014/тпкмашов/Шмелев Дмитрий/Паспорт.jpg](ftp://[redacted]/time500/infa kolya/rabstol/СИБГТУ/5 сессия 2014/тпкмашов/Шмелев Дмитрий/Паспорт.jpg)

регион	проверен	изменен	размер файла
Россия	9 января 2016	21 июля 2014	294.12Kb [301 182 байт]
[похожие файлы] [найти файлы такого же размера] [искать только на этом сервере]			

3. [ftp://\[redacted\]/time500/infa kolya/rabstol/СИБГТУ/5 сессия 2014/тпкмашов/Шмелев Дмитрий/Паспорт \(2\).jpg](ftp://[redacted]/time500/infa kolya/rabstol/СИБГТУ/5 сессия 2014/тпкмашов/Шмелев Дмитрий/Паспорт (2).jpg)



Получение

- Изначально известные данные
- Определение по домену
 - Обход CDN: Cloudfail, etc.
- Поиск по местоположению (Wi-Fi -- BSSID)
 - 3wifi.stascorp.com [1]
- Социальная инженерия
 - IP logging



Использование

- Домен -> Whois [2] GDPR :(
- Местоположение: GeoIP
- Статистика и логи
 - iknowwhatyoudownload.com
- Блэклисты и спам-базы
- Комментарии на сайтах и форумах
- Запущенные сервисы и другое
 - Shodan, Censys, Zoomeye, Fofa, etc.

Пример: нигерийский скам



[1] <http://telegra.ph/Instrukciya-po-opredeleniyu-IP-diapazonov-po-koordinatam-03-18>

[2] <https://medium.com/threat-intel/cybercrime-investigation-insights-bachosens-e1d6312f6b3a>



Что скачивают в интернете с IP 77.71.34.171

Постоянный IP Европа Болгария Варна Geodim Ltd.

Проверь свой IP

У каждого компьютера, подключенного к сети Интернет, есть уникальный адрес. Он состоит из 4х чисел, каждое от 0 до 255, разделенных точками (например 193.91.58.214), и называется IP адресом. IP адрес может быть постоянным (статическим) или изменяться со временем (динамическим).

Выходите в интернет через подключения других людей (через их Wi Fi, компьютеры, планшеты и телефоны) и смотрите на нашем сайте, что они качают, [узнавайте их загрузки через специальную ссылку](#), или смотрите загрузки с "соседних" IP: [77.71.34.149](#) [77.71.34.154](#) [77.71.34.158](#) [77.71.34.162](#) [77.71.34.167](#) [77.71.34.168](#) [77.71.34.171](#) [77.71.34.173](#) [77.71.34.182](#) [77.71.34.187](#)

ПЕРВЫЙ РАЗ (UTC)	ПОСЛЕДНИЙ РАЗ (UTC)	ТИП	НАЗВАНИЕ	РАЗМЕР
3 мая 2019 г., 0:30:29	22 мая 2019 г., 23:47:07	Приложение для PC	kali-linux-2019-1-vm-i386-7z	2.54Гб
3 мая 2019 г., 0:10:04	22 мая 2019 г., 18:29:20	Приложение для PC	kali-linux-2019-1-vm-amd64-7z	2.48Гб

ПОЧТОВЫЕ ЯЩИКИ



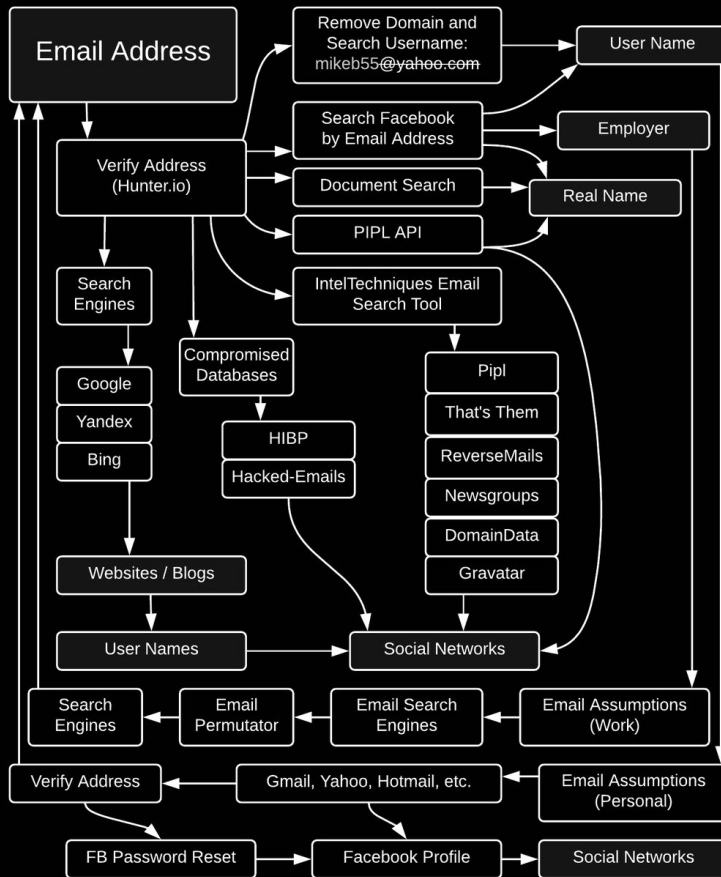
Получение

- Контакты :)
- Whois
- Восстановление доступа к аккаунтам [1]
- Сервисы
 - hunter.io, snov.io
 - haveibeenpwned.com

Использование

- Аккаунты соцсетей, форумов, etc.
 - Резервные ящики, телефоны

Пример: кейс с обманом скаммера



[1] <https://telegra.ph/Kak-ya-po-niknejmu-v-Instagram-nashyol-imya-familiyu-datu-rozhd-eniya-propisku-i-nomer-telefona-ego-vladelca-11-13>



admin@rus-samp.ru

pwned?

Oh no — pwned!

Pwned on 5 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

3 Steps to better security

[Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.






Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 [Subscribe](#) to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

    [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



000webhost: In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Compromised data: Email addresses, IP addresses, Names, Passwords



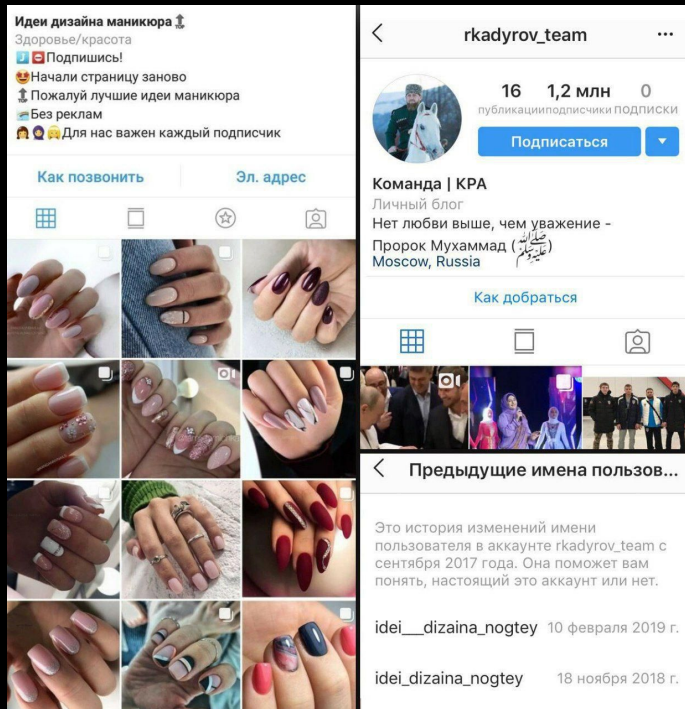
Получение

- Личные данные
- Метаданные
- История изменений
 - В самих сервисах: Steam, etc. [1]
 - Архивные копии

Использование

- Аккаунты
 - Ищем ники по никам [2]
 - usersherlock.com, namechk.com, checkusernames.com
- Упоминания
 - socialmention.com
- Авторство
 - search.buzz.im

Пример: переименование аккаунта



[1] https://t.me/buzzfeed_news/1458

[2] https://pikabu.ru/story/mamkinyi_khakeryi_na_strazhe_nezalezhnosti_6629474



BUZZ.IMTELEGRAM MONITORINGTELEGRAM AD EXCHANGEENG ▾

@soxoj

×

MESSAGES

CHANNELS

AUTHOR

12 ▾

Found 7 results

Inside @In51d3

Спасибо @soxoj , @yoshi_lyosha , ex0dus

Date: 17 May 2019 08:25

Subscribers: 353

Author: In51d3

Технологии и Катан @catans

Участник стрима Soxoj с группой @DC7495 розыгрывает билет на PHDays через поисковой квест, кому интересно залетаем!

Date: 13 May 2019 19:15

Subscribers: 415

Author: catans

RuCTF @ructf

предотвращать атаки на OAuth и SAML и находить уязвимости в разных реализациях OAuth и его аналогов.Сразу после Soxoj [Read more >](#)

Date: 26 Apr. 2019 16:05

Subscribers: 413

Author: ructf

RuCTF [english] @ructf_en

Some technical difficulties, so we've replaced battles with talk about OSINT by soxoj



Получение

- Аккаунты и социальные связи [1]
- Фотографии
- Wikimapia
- Примерное по IP
- Социальная инженерия
 - HTML5 geolocation

Использование

- Поиск по геометкам в соцсетях
 - VK: photo-map.ru, snradar.azurewebsites.net
 - Twitter: onemilliontweetmap.com
 - Youtube: youtube.github.io (self-hosted)
 - Facebook, Flickr, Instagram
- Картографические сервисы
- Региональная специфика

Пример: отслеживание связей террористов, похитителей и скаммеров



[1] <https://medium.com/@benjamindbrown/tracing-syrian-cell-kidnappers-scammers-finances-through-blockchain-e9c52fb6127d>

МЕСТОПОЛОЖЕНИЕ



SnRadar

Главная

О проекте

Укажите точку на карте, требуемый радиус и временной промежуток.
Нажмите кнопку "Найти".
Внизу страницы появятся результаты :)

Широта:

55.759697520115296

Долгота:

37.64710195316057

Радиус:

100

Дата с

24.05.2019

Дата по

25.05.2019

Найти

Марина Ибрагимова

Пол: Женский

25.05.2019 4:20

Александра Вестерберг

Пол: Женский
Возраст: 101

24.05.2019 22:34

Светлана Акимова

Пол: Женский

24.05.2019 21:11

24.05.2019 21:11

24.05.2019 21:11

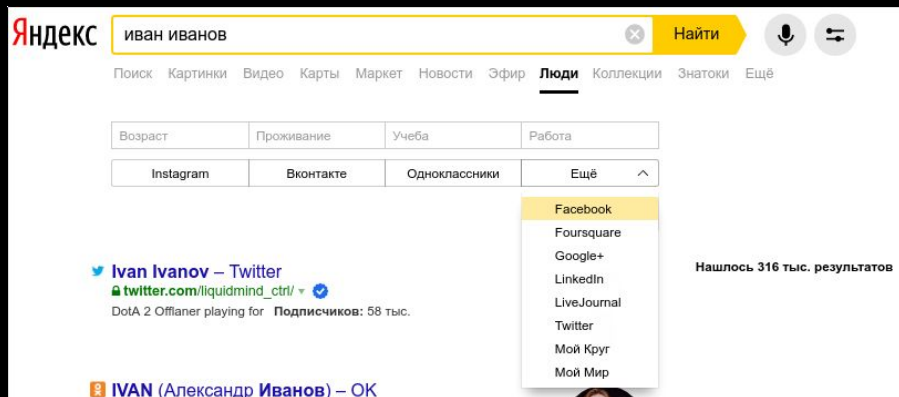


Получение

- Поиск людей
 - Соцсети
 - PeakYou, people.yandex.ru, etc. [1]
- Государственные идентификаторы [2]
 - Учёба: заведение, группа, etc.
 - Транспорт: номер, VIN, etc.
 - Налоги: ИНН, СНИЛС, etc.
 - Бизнес
 - Паспорт

Использование

- Соцсети
 - Другие аккаунты, ящики, телефоны
 - Связи [3]
 - VK: vk.barkov.net, 220vk.com
 - Facebook: graph.tips, stalkscan.com
- Государственные идентификаторы [2]



[1] <https://cumshoat.blogspot.com/2019/04/osint.html>

[2] <https://vas3k.ru/blog/389/>

[3] <https://telegra.ph/Delo-Bogatova-Kto-takoj-Ajrat-Bashirov-05-02>



Поиск по пользователям ВКонтакте

Как работает этот скрипт?

Вы вводите слово, которое есть в имени (фамилии, никнейме или девичьей фамилии) человека, при необходимости уточнения поиска, а скрипт находит подходящих пользователей и выдаёт их список в нужном вам формате.

Это парсинг поиска пользователей ВК. Из-за ограничений VK API список в любом случае ограничен первыми 1000

Показать способ, как найти более 1000 результатов?

1. Слово, которое должно присутствовать в имени или фамилии пользователя:

например, Иван или Иван Иванов

2. Страна или страна+город:

Страна:

----- Любая страна -----

Город:

начните набирать название города...

3. Родной город:

4. Фильтр по полу:

- ☒ Любый пол
☐ Только женщины
☐ Только мужчины

ТЕЛЕФОННЫЙ НОМЕР



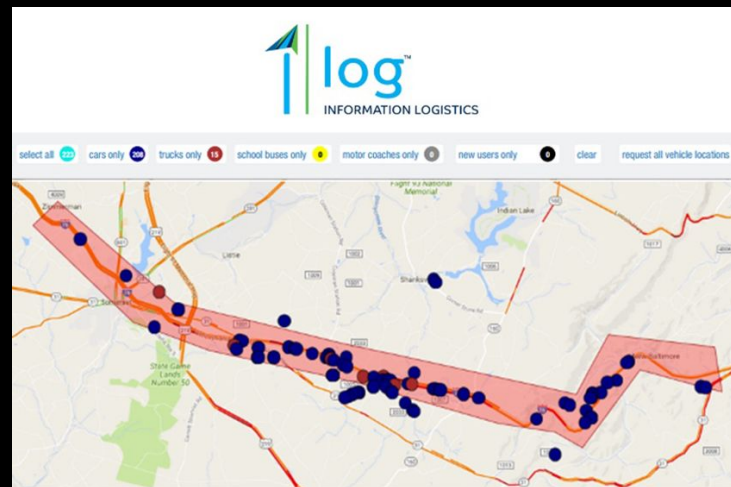
Получение

- Контакты :)
- Whois
- Восстановление доступа к аккаунтам [1]

Использование

- Уточнение имени
 - Мессенджеры [2]
 - Интернет-банки [2]
 - Базы [3, 4]
 - nomer.cc, phonenumber.to
 - GetContact @get_kontakt_bot
- Аккаунты соцсетей, форумов, etc.
 - Синхронизация
 - Прямое получение: Facebook
 - Восстановление доступа

Пример: LocationSmart [5]



[1] <http://web.archive.org/web/20170323165517/http://amdn.news/rassliedovaniie-kto-stoit-za-spinoi-putina-usami-pieskova-surkovskoi-propagandoi-minoborony-roissi-i-mud-roissi>

[2] <https://telegra.ph/Pyatiminutnyj-kejs-po-OSINT-3-03-12>

[3] <https://ftpn.ru/search-phone/>

[4] https://t.me/imonfire_official/41

[5] <https://www.androidauthority.com/locationsmart-tracking-demo-867138/>



PHONE TO NUMBER

Виктор middlename:Викторович carrier:MTC

[Search](#)[Blog](#)[Comments](#)[Stats](#)[Validation tool](#)[Exchange rates](#)[Add phone number](#)[FAQ](#)

Results: 1020679 (0.161 sec.)



Виктор Нарушевич

☎ +3753333365005 📍 Belarus 📶 MTC



Виктор Тарасов Викторович

☎ +79162529812 📍 Москва г, Симферопольский проезд, дом 18, г. Москва и Московская область, Russia, 117638 📶 ПАО "Мобильные ТелеСистемы"



Виктор Виктор

☎ +380500349522 📍 Ukraine 📶 Vodafone



Виктор виктор

☎ +79267798276 📍 г. Москва и Московская область, Russia 📶 ПАО "МераФон"



Виктор Виктор

☎ +79637175190 📍 г. Москва и Московская область, Russia 📶 ПАО "Вымпел-Коммуникации"



Виктор Исаеня

☎ +375295009328 📍 Belarus 📶 MTC



Получение

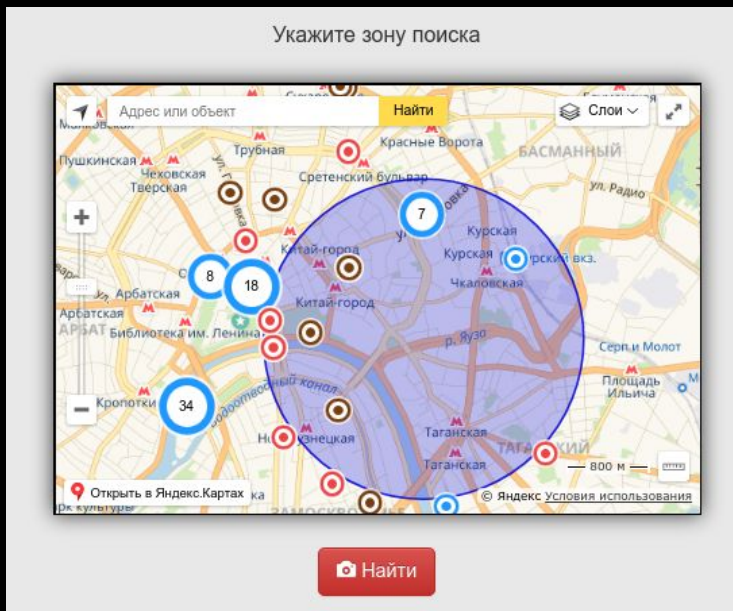
- Аккаунты
- Поиск по местоположению
 - Flickr, Instagram, VK, etc. [1]

Использование

- Поиск по изображениям
 - Google, Yandex, VK, etc. [1]
- Поиск по лицам
 - VK: FindMeVK, FindClone, etc. [1]
 - people.yandex.ru
 - Собственный сервис за полчаса [2]
- Метаданные: EXIF
- Контент

[1] <https://cumshoat.blogspot.com/2019/04/osint.html>

[2] <https://imonfire.xyz/read/post/delaem-svojj-findface-1550974741>





FindMeVK



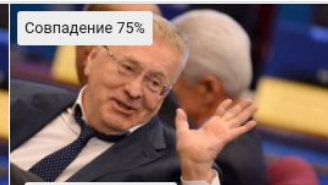
Совпадение 77%

Mike Bolton



Совпадение 76%

Генрих Гимлер



Совпадение 75%

Арсений Трещенко



Совпадение 72%

Павел Мираж



Совпадение 72%

Игорь Титов



100%
БОНУС НА
ПЕРВЫЙ
ДЕПОЗИТ



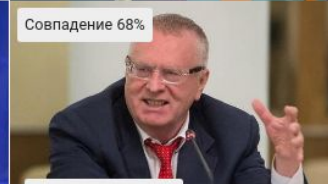
Совпадение 70%

Богдан Ибрагимов



Совпадение 69%

Данил Пивко

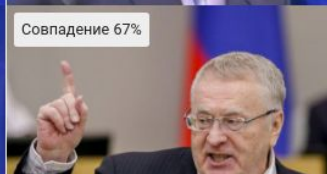


Совпадение 68%

Александр Погодин



Совпадение 68%



Совпадение 67%

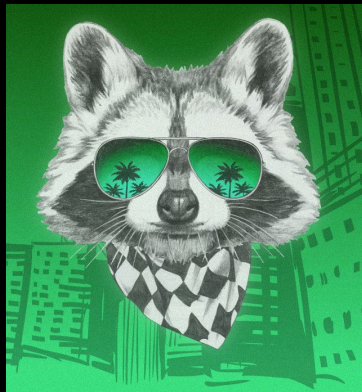


100%
БОНУС НА
ПЕРВЫЙ
ДЕПОЗИТ



Получение

- Облачные хранилища
 - Владельцы
- Файлы
 - Автор и редактор
 - Debug info
 - Альтернативные потоки данных
 - Thumbs.db. .DS_Store
- Git
 - Удалённые файлы
 - Автор и коммитер
- Коды аналитики
 - sameid.net, spyonweb.com



Использование

- Никнеймы и ФИО
- Местоположение
- Дата и время -> Местоположение

“Говорят, здоровый смех продлевает жизнь. Если это в действительности так, то, анализируя полученные образцы стилеров, вирусные аналитики явно выиграли пару-тройку дополнительных лет, ибо смотреть без смеха на подобный чудесный код попросту невозможно” [1]

[1] <https://xakep.ru/2018/05/22/hunting-for-raccoon/>




GitHub, Inc. [US]

github.com/Enot272

FeaturesBusinessExploreMarketplacePricing

Search GitHub

Sign inSign up



Enot272

Enot272

Данное хранилище кода является частной территорией. Кто зайдет без спроса будет в черном в тягчайшей форме. Всем добра!

Block or report user

OverviewRepositories 8Stars 2Followers 10Following 1

Popular repositories

Simple_Stealer_for_Chrome

Простой стилер паролей на Python 2.7; Работает в любой Windows; Браузеры на основе Хромиума.

Python 7 2

Stealer_for_Telegram_Desktop

Стилер для Telegram Desktop; Сливает полностью сессию.

Python 1

LaZagne

Forked from AlessandroZ/LaZagne

Credentials recovery project

Python

enot272.github.io

Simple_Loader

Python

Simple_PyQt4

Python

60 contributions in the last year

MayJunJulAugSepOctNovDecJanFebMarApr

Mon

Wed

Fri

Learn how we count contributions.

LessMore

Contribution activity

Jump to 2018

May 2018

Enot272 has no activity yet for this period.

April 2018

Created 1 commit in 1 repository

ПРОФИЛЬ ПОЛЬЗОВАТЕЛЯ

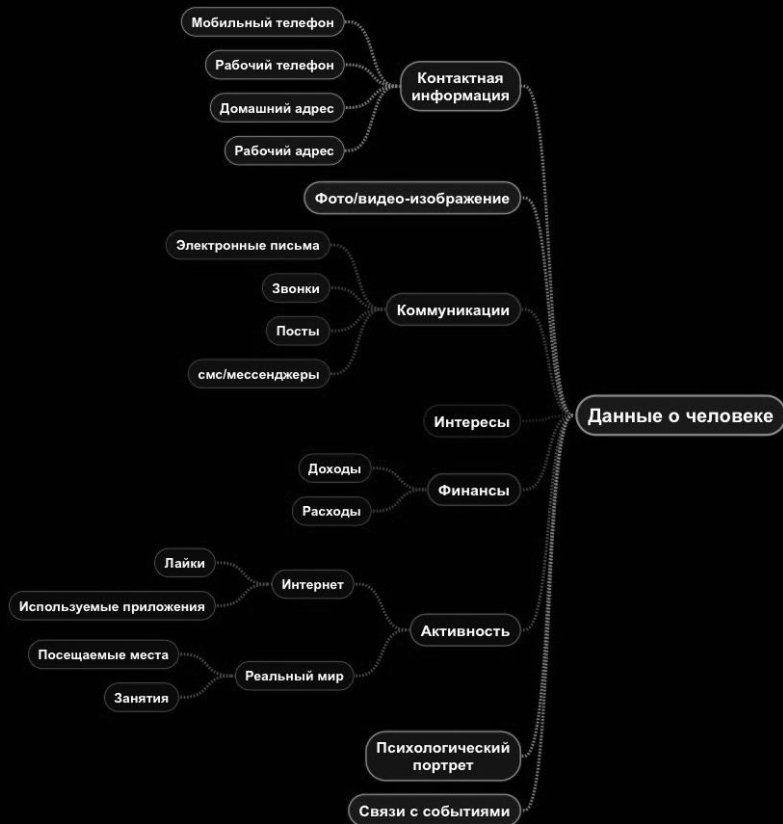


Получение

- Аккаунты: базовая информация, посты
- Сопоставление
 - Стилometрия [1]
 - Голос [2]
 - Статус онлайн [3]

Использование

- Психологический портрет и интересы
 - Продажа
 - Реклама
 - Влияние на общественное мнение (Cambridge Analytica)
 - Разбор внутренних инцидентов



[1] <https://xakep.ru/2013/01/10/59921/>

[2] <https://habr.com/ru/post/144491/>

[3] <https://www.securitylab.ru/analytics/490726.php>



- Парсеры и агрегаторы
 - Instagram, VK, Авито, etc.
- Хранение копий и ссылок
 - web.archive.org, archive.is [1]
 - Hunchly
- Системы версионирования
- Мониторинг
- Авторизация на ресурсах

Пример: отслеживание миграций мошенников



[1] <https://habr.com/ru/company/echelon/blog/321754/>

УТЕЧКИ БАЗ ДАННЫХ



- Любые пользовательские данные -- товар
 - Не люди, а **лиды**
- Агрегация самых разных данных
 - Все мыслимые схемы пробива
- Поиск и индексация общедоступных БД давно поставлены на поток [1]
- Инструменты
 - `haveibeenpwned.com`
 - `databases.today`



[1] <https://t.me/dataleak>



Подборки

- <https://osintframework.com/>
- <https://github.com/OldBonhart/Osint-Resources>
- <https://github.com/netstalking-core/netstalking-osint>
- <https://github.com/Ph055a/OSINT-Collection>
- <https://github.com/jivoi/awesome-osint>
- https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf

Агрегаторы

- RISKIQ
- Lampyre.io
- Maltego
- SpiderFoot
- theHarvester
- Datasplloit



The End

СПАСИБО. ВОПРОСЫ?