



OSINT

КОНКУРЕНТНАЯ РАЗВЕДКА

Namech_k

Что такое конкурентная разведка?

- сбор и обработка данных из открытых источников

Где применяется?

- Сбор компанией информации о конкурентах
- Расследование киберинцидентов
- Подготовка информации для проведения тестирования на проникновение

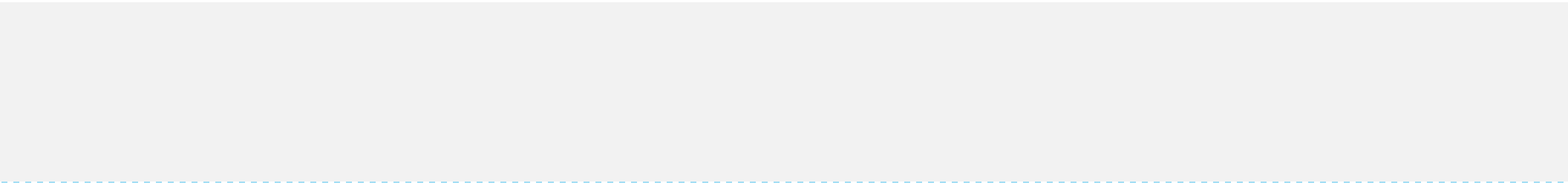
ПОИСКОВИКИ



Google: операторы языка запросов

- `info:site.org` – получение сведений о сайте
- `site:site.org` — поиск по всем поддоменам и страницам указанного сайта
- `cache:site.org` – поиск кешированной версии сайта
- `related:site.org` – поиск сайтов с похожим контентом
- Исключение результатов с определенными словами – слово1 –слово2
- Поиск точного слова или фразы – «фраза для поиска»
- И т.д. (см. список в конце)

Сбор информации различных IoT-устройств



Ресурсы

➤ shodan.io

- Имеется API
- Имеется CLI

➤ censys.io


- Имеется API


Сбор информации о WEB-ресурсе



-
- Регистрационная информация: WHOIS, история регистрации домена, reverse IP и др.
 - История сайта: cache, веб-архивы (<http://archive.org/web>, <http://archive.is>)
 - Анализ адресной строки
 - Технический анализ сайта: перебор директорий (DirBuster) и поддоменов сайта (SubBrute), анализ Robots.txt и т.д.
 - Сетевое сканирование, поиск (и эксплуатация) уязвимостей

WHOIS





[Premium Domains](#)

[Transfer](#)

[Features](#)

itsecwiki.org

whois information

Whois

History

DNS Records

Diagnostics

cache expires in 23 hours, 56 minutes and 1 seconds

Registrar Info

Name	eNom, Inc.
Referral URL	http://www.enom.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2018-10-06
Registered On	2015-10-06
Updated On	2017-09-07

Name Servers

DNS1.NAMECHEAPHOSTING.COM	216.87.155.33
DNS2.NAMECHEAPHOSTING.COM	216.87.152.33

Similar Domains

Карты



Wikimapia

Может быть полезно:

- Название объекта
- Координаты
- Описание и обсуждение объекта участниками сообщества
- Фотографии
- Категории

Google/Yandex карты

Что может быть полезно:

- Поиск по координатам
- Вид со спутника
- Панорамы

Социальные сети



Профиль пользователя

Какие есть способы найти другие аккаунты пользователя?

1. Информация в профиле – никнеймы, ссылки на другие страницы, e-mail, и т.п.
2. Фотография профиля – одинаковые фотографии профилей в разных соцсетях (поиск по картинкам Google)
3. Поиск по никнейму в других соцсетях (<https://namechk.com/>)
4. Построение социального графа друзей, выявление кругов общения (API соцсети)

Документы пользователя

- Имя создателя файла
- Дата создания файла
- Служебная информация редактора
- Имя компьютера, на котором создан файл

Фотографии пользователя

- Геометки
- Дата создания
- Содержание фото
- Отметки людей на фото

Полезные ссылки

Поисковые запросы:

- <https://support.google.com/websearch/answer/2466433?hl=ru>
- <http://aiwaspb.ru/prodvizhenie/operatory-poiskovykh-sistem.html>
- <https://semantica.in/blog/yazyk-zaprosov-poiskovykh-sistem-yandeks-i-google-asdfq.html>

Полезные ссылки

API социальных сетей:

- VK: <http://vk.com/dev>
- Instagram: <https://www.instagram.com/developer/>
- Facebook: <https://developers.facebook.com/docs/>

Много полезных ссылок

<https://github.com/jivoi/awesome-osint>