

# OSINT или разведка по открытым источникам / Хабр

 [habr.com/ru/companies/deiteriylab/articles/595801](https://habr.com/ru/companies/deiteriylab/articles/595801)

kukuxumushi



[kukuxumushi](#) 16 дек 2021 в 19:16

## OSINT или разведка по открытым источникам

26 мин

140K



Поиск по открытым источникам — это методология сбора и анализа данных, находящихся в открытом доступе, для получения дополнительной информации о цели.

В данной статье расскажем о том, какими методами и средствами можно собирать информацию из открытых источников об организации, покажем примеры такой информации и расскажем о максимально большом количестве утилит и методов, которые могут помочь увеличить покрытие.

Надеемся, что статья будет полезна как пентестерам и охотникам за ошибками для увеличения области аудита, так и стороне защиты (blue team, application security и т.д.) для защиты инфраструктуры своей организации.

### Дисклеймер

В рамках статьи, понятия OSINT, open-source intelligence, recon, reconnaissance, рекогносцировка и поиск по открытым источникам будут синонимами.

В статье приведены только бесплатные программы, с открытым исходным кодом и программы с пробным периодом.

## С чего все начинается

---

Самым первым этапом проведения пентеста (после заключения договора) является выделение области тестирования и сбор информации о цели. В зависимости от специфики конкретного пентеста количество изначальных сведений может отличаться, однако, предполагается, что на данном этапе мы знаем:

- Название организации.
- Род деятельности организации.
- Доменное имя организации.

Что можно получить благодаря поиску в интернете?

- Из одного домена сделать множество доменов и поддоменов.
- Найти новые точки входа.
- Найти интересные пути в веб-приложениях и API.
- Получить информацию об используемом ПО, аппаратных компонентах и используемых языках программирования.
- Найти учетные записи, которые могут быть активными в целевых веб-приложениях.
- Найти уязвимости.

## OSINT workflow\mindmap

---

Казалось бы, что пользоваться поисковыми системами умеет каждый, но при этом множество исследователей пишут огромные статьи и майндмапы как они эффективно ищут в интернете. Например, по [ссылке](#) доступна подборка таких майндмапов. Подборке уже несколько лет, но она все еще остается актуальной.

Стоит заметить, что осинт это циклический процесс: если мы находим какую-либо информацию, например, новый IP адрес или доменное имя, то для них надо проделать все те же шаги, которые мы прошли, чтоб их найти.

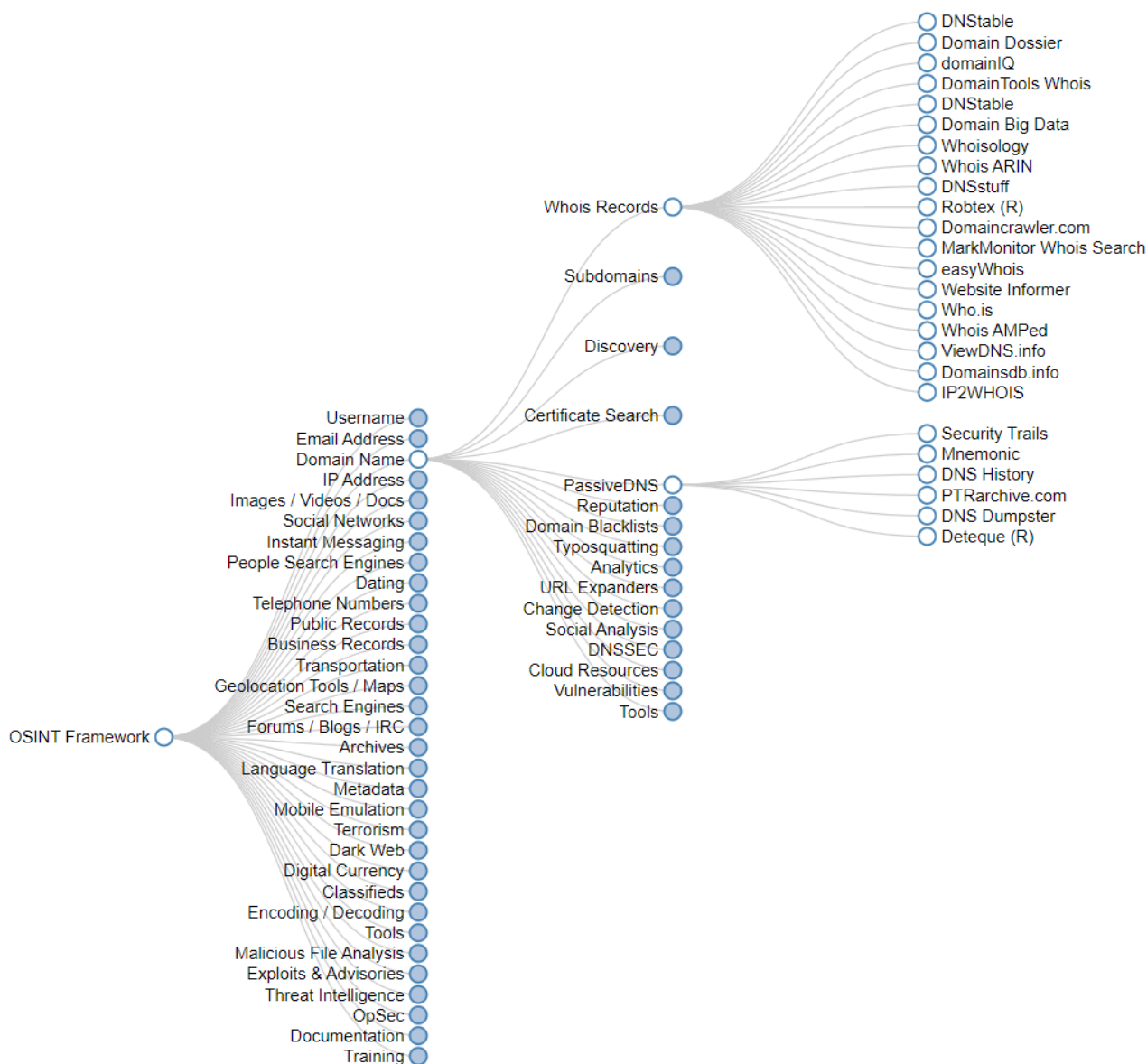
## OSINT Framework

---

Самый популярный майндмап для поиска по открытым источникам это [OSINT Framework](#).

Его прелесть в том, что он вобрал в себя всевозможные сайты, утилиты и базы данных, которые могут быть полезны при рекоме. На любой ваш вопрос по осинту, скорее всего, в нем будет ответ.

Единственный минус в том, что он сделан для стран наподобие США, и он не учитывает, что в России своя специфика.



## Активная и пассивная разведка

Рекон подразделяется на 2 этапа: пассивная и активная разведка.

### Пассивная разведка

Во время пассивной разведки вы никак не взаимодействуете с вашей целью. Вы не отправляете ей пакеты со своего компьютера, вы не резолвите доменные имена на серверах цели, вы не пингуете ее айпишники, вы не заходите на ее веб-приложения, и даже двери офиса не трогаете.

Примеры данного этапа разведки:

Поиск в поисковых системах типа Google и "хакерских" поисковых системах, просмотр баз данных с утечками, анализ вакансий на [HH](#) и [linkedin](#), извлечение метаданных из публично доступных файлов и т.д.

## Активная разведка

---

Взаимодействие с инфраструктурой организации: скан портов, перебор директорий, запуск "шумных" сканеров (Acunetix, Burp Pro Active Scanner и т.д.), фаззинг параметров, резолвинг большого количества доменных имен на серверах цели и т.д.

Такие действия создают много логов в SIEM-системах, триггеров в SOC и могут даже положить несколько серверов.

В данной статье будет затронута только тема пассивной разведки.

## Начинаем разведывать

---

Давайте для начала вспомним про самые популярные записи DNS, которые могут быть нам полезны:

- A запись — соответствие домена IPv4-адресу.
- AAAA запись — соответствие домена IPv6-адресу.
- CNAME — Canonical name — используется для того, чтобы один домен мог указывать на другое имя домена.
- MX — Mail Exchange — адрес почтового сервера.
- TXT — большая текстовая строка длиной 65535 байт. Используется для публичных ключей, SPF, и другой информации.
- NS — Name Server — указание на сервер резолвинга доменных имен.
- SOA — Start of Authority — информация об администраторе домена. Используется при делегировании домена. В записи содержится Name Server, ответственное лицо и таймстемпы, относящиеся к срокам делегирования.
- PTR — Pointer — содержит IP-адрес, который указывает на домен при reverse DNS lookup (обратном резолвинге).

A	@	→	64.227.77.243
AAAA	@	→	7628:0d18:11a3:09d7:1f34:8a2e:07a0:765d
MX	mail.ru	→	mailexchange.doyouwannaseestudentmagic.space. 0
NS	t	→	tunnel.doyouwannaseestudentmagic.space. 0
TXT	@	→	mailru-domain: 9dBXyDRfGJvLIn6l

Пример некоторых DNS записей

## Доменные имена

---

Самое первое и простое что мы можем сделать — это порезолвить доменные имена. Для этого есть десятки утилит, как терминальных так и доступных онлайн.

Неполный список утилит и сервисов, которые могут разрезолвить доменное имя:

Selfhosted:

- Nslookup (linux\windows nslookup yandex.ru).
- Ping (linux\windows ping yandex.ru).
- Traceroute (linux traceroute ya.ru \ windows tracert ya.ru).
- Dig (linux dig @8.8.8.8 yandex.ru ANY).
- Host (linux host yandex.ru).
- getent (linux getent hosts yandex.ru).
- resolveip (linux resolveip -s yandex.ru).
- Resolve-DnsName (windows Resolve-DnsName -Name yandex.ru).

```

root@MSI:/# nslookup yandex.ru
Server:      172.29.144.1
Address:     172.29.144.1#53

Non-authoritative answer:
Name:   yandex.ru
Address: 77.88.55.77
Name:   yandex.ru
Address: 77.88.55.88
Name:   yandex.ru
Address: 5.255.255.80
Name:   yandex.ru
Address: 5.255.255.88
Name:   yandex.ru
Address: 2a02:6b8:a::a

```

```
PS C:\> Resolve-DnsName yandex.ru
```

Name	Type	TTL	Section	IPAddress
yandex.ru	AAAA	91	Answer	2a02:6b8:a::a
yandex.ru	A	116	Answer	5.255.255.88
yandex.ru	A	116	Answer	5.255.255.80
yandex.ru	A	116	Answer	77.88.55.88
yandex.ru	A	116	Answer	77.88.55.77

```
PS C:\>
```

```
C:\>ping -n 1 yandex.ru
```

```

Pinging yandex.ru [5.255.255.80] with 32 bytes of data:
Reply from 5.255.255.80: bytes=32 time=19ms TTL=55

```

```

root@MSI:/# host yandex.ru
yandex.ru has address 5.255.255.88
yandex.ru has address 77.88.55.77
yandex.ru has address 77.88.55.88
yandex.ru has address 5.255.255.80
yandex.ru has IPv6 address 2a02:6b8:a::a
yandex.ru mail is handled by 10 mx.yandex.ru.

```

```
C:\>tracert yandex.ru
```

```
Tracing route to yandex.ru [77.88.55.88]
```

Вывод различных утилит для резолва доменных имен

Online:

<https://dns.google.com>

► Пример результата работы веб-приложения

[https://www.dnsqueries.com/en/dns\\_lookup.php](https://www.dnsqueries.com/en/dns_lookup.php)

► Пример результата работы веб-приложения

<https://whatismyipaddress.com/hostname-ip>

► Пример результата работы веб-приложения

<https://dnschecker.org/all-dns-records-of-domain.php>

► Пример результата работы веб-приложения

<https://check-host.net/check-dns>

► Пример результата работы веб-приложения

<https://bgp.he.net/>

► Пример результата работы веб-приложения

**Что это нам дает?**

Помимо соответствия IP-адрес—домен мы можем узнать, например, DNS-серверы, с помощью утилиты nslookup, а также можем получить все DNS-записи, например, командой dig.

```

root@MSI:/# nslookup -type=ns yandex.ru
Server:          172.29.144.1
Address:         172.29.144.1#53

Non-authoritative answer:
yandex.ru       nameserver = ns2.yandex.ru.
yandex.ru       nameserver = ns9.z5h64q92x9.net.
yandex.ru       nameserver = ns1.yandex.ru.

```

Получение NS Записей доменного имени yandex.ru утилитой nslookup

```

root@MSI:/# dig @8.8.8.8 yandex.ru ANY
;; ANSWER SECTION:
yandex.ru.      3447    IN      SOA     ns1.yandex.ru. sysadmin.yandex-team.ru. 2021121148 600 300 2592000 900
yandex.ru.      3447    IN      CAA     0 issuewild "globalsign.com"
yandex.ru.      3447    IN      CAA     0 issue "globalsign.com"
yandex.ru.      3447    IN      CAA     0 issue "yandex.ru"
yandex.ru.      3447    IN      CAA     0 issuewild "yandex.ru"
yandex.ru.      1047    IN      TXT     "MS=ms75457885"
yandex.ru.      1047    IN      TXT     "v=spf1 redirect=_spf.yandex.ru"
yandex.ru.      1047    IN      TXT     "b7e95449ad0a156bb6f5135a88af4d2ff4abde2a8ald336351cf68e36ffdedfb"
yandex.ru.      1047    IN      TXT     "_globalsign-domain-verification=LD5-OgV_QE93G8rzNaeJKvtqe9t1P5AZtyDodrld
Yh"
yandex.ru.      1047    IN      TXT     "have-i-been-pwned-verification=13c7b50cd0b12f85dabe796e6178fb74"
yandex.ru.      1047    IN      TXT     "2e35680fa5ac784cf58decal80385b5eff74dfef831c2d73830425e8a8deb7d5"
yandex.ru.      1047    IN      TXT     "mailru-verification: 530c425b1458283e"
yandex.ru.      1047    IN      TXT     "e586105d5a91ebdc106bd3936137e25441ffaaa30a930a5b1a1114c10140cf9"
yandex.ru.      1047    IN      TXT     "google-site-verification=XyQD85000-0rTv33yw7AX-EiuH1vSyW5PjkYeYxxPEg"
yandex.ru.      1047    IN      TXT     "facebook-domain-verification=e750ewnm68u4f83wvp6qp7iiphkj0"
yandex.ru.      147     IN      MX      10 mx.yandex.ru.
yandex.ru.      21447   IN      NS      ns1.yandex.ru.
yandex.ru.      21447   IN      NS      ns9.z5h64q92x9.net.
yandex.ru.      21447   IN      NS      ns2.yandex.ru.
yandex.ru.      147     IN      A       5.255.255.70
yandex.ru.      147     IN      A       77.88.55.55
yandex.ru.      147     IN      A       77.88.55.70
yandex.ru.      147     IN      A       5.255.255.5
yandex.ru.      147     IN      AAAA    2a02:6b8:a::a

```

Получение всех записей для доменного имени yandex.ru утилитой dig

Имея IP-адреса веб-приложений мы можем начать смотреть соседние IP-адреса в подсетях, перебирать виртуальные хосты и изучать владельцев этих IP-адресов.

DNS-серверы нам могут в дальнейшем помочь при активной разведке для перебора поддоменов и проведения различных атак.

## Whois

Whois — протокол, основная цель которого заключается в получении регистрационных данных о владельцах доменных имён, IP-адресах и автономных систем (ASN).

Изначально целью появления системы Whois было дать возможность системным администраторам искать контактную информацию других администраторов серверов по IP-адресам и доменным именам.

Неполный список утилит и сервисов, которые могут показать содержимое Whois:

- Whois (windows/linux whois [yandex.ru](#) и whois 77.88.55.77)



- <https://whois.ru/>

► Пример результата работы веб-приложения

<https://dnschecker.org/ip-whois-lookup.php>

► Пример результата работы веб-приложения

<https://bgp.he.net/>

► Пример результата работы веб-приложения

## Что это нам дает?

Из вывода Whois можно получить email-адреса владельцев и администраторов, адреса DNS-серверов, подсети и ASN.

```
root@DESKTOP-5MMIEVF:/# whois yandex.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain:            YANDEX.RU
nserver:           ns1.yandex.ru. 213.180.193.1, 2a02:6b8::1
nserver:           ns2.yandex.ru. 93.158.134.1, 2a02:6b8:0:1::1
nserver:           ns9.z5h64q92x9.net.
state:             REGISTERED, DELEGATED, VERIFIED
org:               YANDEX, LLC.
registrar:         RU-CENTER-RU
admin-contact:     https://www.nic.ru/whois
created:           1997-09-23T09:45:07Z
paid-till:         2022-09-30T21:00:00Z
free-date:         2022-11-01
source:            TCI

Last updated on 2021-12-05T22:01:30Z
```

Вывод утилиты whois для доменного имени yandex.ru



```
root@DESKTOP-5MMIEVF:/# whois 77.88.55.77
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '77.88.55.0 - 77.88.55.255'

% Abuse contact for '77.88.55.0 - 77.88.55.255' is 'abuse@yandex.ru'

inetnum:        77.88.55.0 - 77.88.55.255
netname:        YANDEX-77-88-55
status:         ASSIGNED PA
country:        RU
descr:          Yandex enterprise network
admin-c:        YNDX1-RIPE
tech-c:         YNDX1-RIPE
remarks:        INFRA-AW
mnt-by:         YANDEX-MNT
created:        2012-10-12T12:22:03Z
last-modified:  2014-03-26T08:17:12Z
source:         RIPE

role:           Yandex LLC Network Operations
address:        Yandex LLC
address:        16, Leo Tolstoy St.
address:        119021
address:        Moscow
address:        Russian Federation
phone:          +7 495 739 7000
fax-no:         +7 495 739 7070
```

Вывод утилиты whois для IP-адреса 77.88.55.77

## Whois history

---

Существуют сервисы периодически собирающие и агрегирующие записи Whois. Благодаря таким сервисам можно поностальгировать и получить использующиеся ранее почты, хостинги, DNS-серверы и целые подсети:

<http://whoishistory.ru/>

Сервис заброшен, расширенный поиск не работает, но все еще можно получить историю по имени домена в зонах .ru и .рф (пока не вылезет капча)

► Пример результата работы веб-приложения

<https://tools.whoisxmlapi.com/whois-history-search>

► Пример результата работы веб-приложения

## Reverse Whois

---

Тогда как Whois выдает сведения по доменным именам или IP-адресам, обратный Whois позволяет искать по всей информации, которая есть в выводе обычных Whois, например, по email-адресам, по именам владельцев, по организациям и т.д.

Таким образом можно расширить скоуп найдя новые email-адреса, хостинги, DNS-серверы, подсети, доменные имена и поддомены.

Неполный список сервисов, которые могут искать по содержимому Whois:

<https://www.reversewhois.io/>

► Пример результата работы веб-приложения

<https://viewdns.info/reversewhois>

► Пример результата работы веб-приложения

## Что это нам дает?

Поиск по содержимому Whois позволяет находить забытые администраторами веб-приложения и сервисы, особенно, если использовать его вместе в поиском по истории Whois.

Также можно обнаружить:

- Email-адреса.
- Хостинг-провайдеров.
- DNS-серверы.
- Подсети.
- Домены и поддомены.

## SPF и DMARC

---

SPF и DMARC нужны для отправки и приема почты, а в частности для того чтобы злоумышленники от вашего имени не отправляли письма.

SPF — это подпись, содержащая информацию о серверах, которые могут отправлять письма. В SPF используются свои правила и синтаксис. В том числе, в ней содержатся IP-адреса и доменные имена.

DMARC — это политика, которая показывает как обращаться с письмами, которые пришли не с доменов указанных в SPF.

Неполный список утилит для поиска и анализа SPF и DMARC:

SPF:

<https://mxtoolbox.com/spf.aspx>

► Пример результата работы веб-приложения

<https://www.dmarcanalyzer.com/spf/checker/>

- ▶ Пример результата работы веб-приложения

<https://dmarcian.com/spf-survey/>

- ▶ Пример результата работы веб-приложения

DMARC:

<https://mxtoolbox.com/DMARC.aspx>

- ▶ Пример результата работы веб-приложения

<https://dmarcian.com/dmarc-inspector/>

- ▶ Пример результата работы веб-приложения

Для анализа SPF также есть selfhosted утилита, которая извлекает поддомены из SPF записей <https://github.com/0xbharath/assets-from-spf>.

- ▶ Пример запуска и результат работы утилиты

## IP и подсети

---

### Reverse DNS lookup

---

Обратный резолв DNS-адресов — поиск по PTR записям DNS. Если администратор добавил такую запись, то по IP-адресу можно будет узнать, какие доменные адреса на него указывают.

Неполный список сервисов, которые могут провести Reverse DNS lookup:

<https://check-host.net/check-dns>

- ▶ Пример результата работы веб-приложения

<https://dnschecker.org/ip-to-hostname.php>

- ▶ Пример результата работы веб-приложения

<https://mxtoolbox.com/ReverseLookup.aspx>

- ▶ Пример результата работы веб-приложения

<https://dnschecker.org/reverse-dns.php>

- ▶ Пример результата работы веб-приложения

**Что это нам дает?**

В приложениях часто используется роутинг на основании имени хоста (vhosts), поэтому зная только IP-адрес, мы попадем на страницу ошибки веб-сервера, а с помощью Reverse DNS lookup можно получить имя хоста и добраться к самому веб-приложению.

## DNS history

---

История DNS записей домена. Существуют сервисы, которые запоминают записи DNS, и показывают их историю.

Сервис <https://viewdns.info/iphistory>, запоминает только A записи доменов и дату привязки.

► Пример результата работы веб-приложения

А сервис <https://securitytrails.com/>, помимо A записи, позволяет искать также по AAAA, MX, NS, SOA и TXT записям.

► Пример результата работы веб-приложения

### Что это нам дает?

Это позволяет расширить область аудита, узнав новые IP-адреса, а также получить:

- DNS-серверы.
- Доменные имена.
- Почтовые серверы.

Если узнать IP-адреса, которые использовались ранее, тогда можно даже обойти Web Application Firewall. Поиск старых IP-адресов, например, один из методов обхода защиты Cloudflare.

Помимо приведенных выше веб-сервисов можно также воспользоваться selfhosted решениями:

<https://github.com/MrH0wl/Cloudmare>

► Пример запуска и результат выполнения утилиты

<https://github.com/m0rtem/CloudFail> (проект сейчас мертв, но, надеемся, что скоро его оживят)

## ASN lookup

---

ASN (autonomous system number) — номер автономной системы.

Интернет состоит из локальных сетей, каждая из которых имеет подсети и свои политики маршрутизации, и которые соединяются с другими локальными сетями. Одна такая локальная сеть, это одна автономная система и у нее есть уникальный номер — ASN. Эти номера используются в BGP-маршрутизации.

По номеру AS можно посмотреть IP-адреса и подсети, которые в ней содержатся. Если это большая компания, типа Яндекса, или университетов, то можно предположить что вся AS принадлежит этой компании, и большая ее часть, может войти в область аудита. Также в выводе можно обнаружить почтовые адреса и другую информацию о компании.

Неполный список сервисов, которые имеют возможность поиска по ASN:

<https://bgp.he.net/>

► Пример результата работы веб-приложения

<https://ipinfo.io/>

► Пример результата работы веб-приложения

<https://viewdns.info/asnlookup/>

► Пример результата работы веб-приложения

## Поисковые системы

---

### Как гуглить?

---

Вы каждый день пользуетесь поисковиками типа Google или Яндекс, но, наверное, не все подозревают, что умеет этот самый Google.

Используя немного магии поиска можно получить множество полезной информации.

### Что можно получить из поисковой системы?

- Поддомены.
- Диапазоны IP-адресов.
- Информацию об утечках учетных данных.
- Комментарии в исходном коде.
- Веб-страницы для разработчиков (например dev.\*).
- Файлы и страницы, содержащие секреты и пароли.
- Карты веб-сайтов.
- Закэшированные страницы.
- Потенциально опасные файлы.
- URL-адреса и пути, которые могут являться точками входа.

- Другие ресурсы, связанные с организацией.

## Как искать?

Для поиска нужно использовать специальные операторы. Например, список операторов для Google:

- “” — точное совпадение.
- — исключить из поиска.
- Логические операторы: &, ||.
- Site:itmo.ru — поиск в пределах сайта.
- cache:itmo.ru — возвращает кэш сайта.
- filetype:txt — только txt файлы.
- related:itmo.ru — сайты связанные с искомым.
- inurl:test — в URL встречается слово test.
- intitle:test — в Title встречается слово test.
- intext:test — в тексте встречается слово test.

В других поисковых системах список операторов может отличаться.

По продвинутому использованию поисковиков существует множество статей, поэтому не будем углубляться в эту тему:

- <https://www.exploit-db.com/google-hacking-database> — подборка готовых полезных нагрузок для поиска Google.
- <https://habr.com/ru/post/437618/> — полный список операторов поиска Google.
- <https://yandex.ru/support/search/query-language/search-operators.html> — документация по поиску в Яндекс.
- [https://www.tutorialspoint.com/google\\_hacking\\_tests.htm](https://www.tutorialspoint.com/google_hacking_tests.htm) — однокнопочное решение для поиска: вводите домен, нажимаете на нужную кнопку и получаете вывод Google.

► Пример результата работы веб-приложения

[http://www.googleguide.com/advanced\\_operators\\_reference.html](http://www.googleguide.com/advanced_operators_reference.html).

## Поисковые системы для хакеров

---

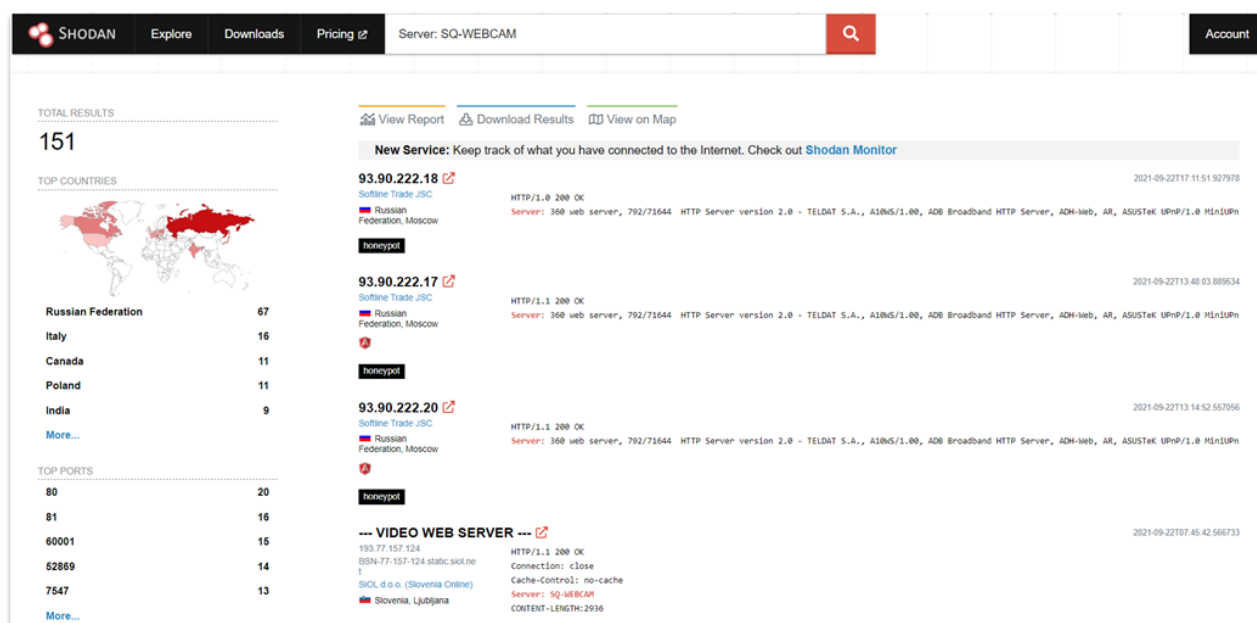
Помимо поиска в обычных поисковых системах типа Google можно искать в специальных "хакерских" поисковых системах. Примеры таких поисковиков:

- <https://www.shodan.io/>
- <https://censys.io/>
- <https://www.binaryedge.io/>

Эти сервисы постоянно сканируют весь интернет, и заполняют свои базы ответами серверов.

Все приведенные выше сервисы имеют платные функции, но без покупки подписки можно получить ограниченный вывод, ограниченную функциональность или ограниченное количество запросов в месяц.

## Shodan



shodan.io — поиск серверов SQ-WEBCAM

Сервис позволяет искать по IP-адресам, портам и содержимому ответов сервера. Это может позволить найти новые поддомены, а также то, что не смог найти Nmap.

Для поиска используется свой синтаксис, с которым можно ознакомиться по ссылке <https://help.shodan.io/the-basics/search-query-fundamentals>.

## Censys



censys.io — поиск FTP-серверов в России со словом yandex в теле ответа

Censys этот тот же самый Shodan, но более новый и с приятным интерфейсом.

Опять же используется свой синтаксис, с которым можно ознакомиться по ссылке: <https://search.censys.io/search/language>.

## Binaryedge

Еще более новая разработка это сервис BinaryEdge.

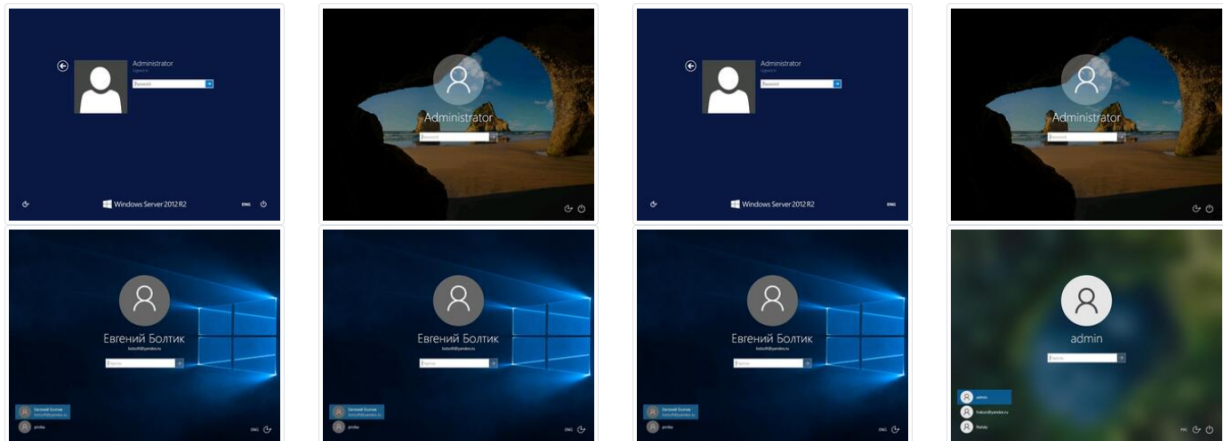
binaryedge.io — поиск поддоменов для доменного имени yandex.ru

Помимо тех же функций, которые имеются и в Shodan и в Censys, данный сервис еще умеет искать поддомены, email-адреса в утечках данных, умеет искать изображения, связанные с доменом, и в этих картинках умеет искать по тексту.

Results for your query: *yandex.ru*  
38 results found.

Showing 1 to 20 of 38 entries.

1 2



binaryedge.io — поиск по изображениям для доменного имени yandex.ru

В сервисе есть еще несколько различных функций, но они уже недоступны в бесплатных и пробных версиях.

Документация с примерами доступна по ссылке: <https://docs.binaryedge.io/search/>.

## Метаданные

Каждый раз, когда вы создаете или редактируете файл, в нем остается множество метаданных. Когда вы загружаете этот файл в интернет, зачастую метаданные сохраняются. Так как поисковые системы индексируют файлы, вы можете найти их, например, в google используя оператор поиска file.

Существуют уже готовые решения, которые позволяют ввести домен, выбрать интересные расширения файлов и ожидать результатов:

<https://github.com/laramies/metagoofil>

► Пример запуска и результат выполнения утилиты

<https://github.com/ElevenPaths/FOCA>

► Пример запуска и результат выполнения утилиты

## Что нам это дает?

- Email-адреса
- ФИО сотрудников
- Используемое ПО
- Используемые операционные системы
- IP-адреса

- Поддомены

## Системы контроля версий

Системы контроля версий (github, gitlab и т.д.) также обладают возможностями расширенного поиска. У них свой синтаксис и свои "дорки".



Поиск слова password в файлах secrets.yml в системе контроля версий github.com

### Что нам это дает?

- Пароли и секреты.
- Части кода приложений.

Несколько полезных ссылок для поиска по коду:

<https://publicwww.com/> — ищет по фронтенд-коду веб-сайтов. Документация по синтаксису <https://publicwww.com/syntax.html>.

► Пример результата работы веб-приложения

<https://searchcode.com/> — ищет по опубликованному исходному коду в публичных системах контроля версий.

► Пример результата работы веб-приложения

<https://github.com/techgaun/github-dorks> — полезная информация по операторам поиска на github.

Также есть несколько selfhosted сервисов для поиска секретов на github:

<https://github.com/eth0izzle/shhgit>

► Пример запуска и результат выполнения утилиты

<https://github.com/michenriksen/gitrob>

► Сведения об установке, пример запуска и результат выполнения утилиты

<https://github.com/zricethezav/gitleaks>

Утилита ищет секреты в репозиториях на файловой системе.

► Пример запуска и результат выполнения утилиты

Также, если мы нашли никнеймы и email-адреса сотрудников, мы можем поискать их аккаунты в различных системах контроля версий, и посмотреть, что они коммитят. Потенциально возможно найти в личных репозиториях сотрудников части кода приложений компании-цели.

Также, стоит заметить, что нужно анализировать не только последнюю версию исходного кода в ветке master, но и предыдущие коммиты. Сотрудник может закоммитить критичные данные в систему контроля версий, понять, что он "накосячил" и удалить их следующим коммитом. Не удалив сам коммит из истории.

### Что еще можно получить из систем контроля версий?

Gitlab имеет возможность перечисления пользователей по URL-адресам вида: <https://gitlab.com/api/v4/users/1>, где 1 это порядковый номер пользователя. В selfhosted версиях gitlab такая уязвимость тоже присутствует.

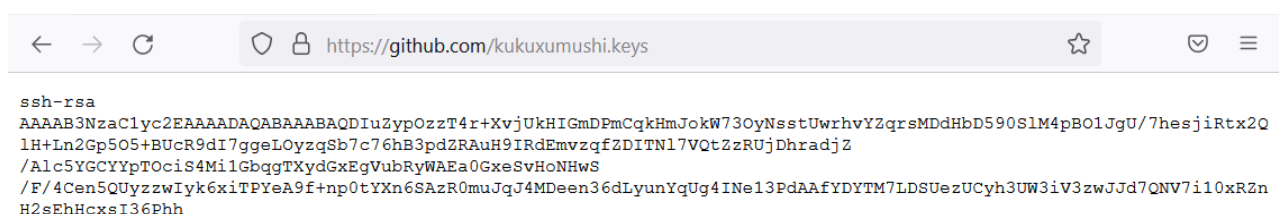
```
{ "id": 1, "username": "sytses", "name": "Sid  
Sijbrandij", "state": "active", "avatar_url": "https://secure.gravatar.com/avatar/78b060780d36f51a6763ac9831a4f022?  
s=80&u0026d=identicon", "web_url": "https://gitlab.com/sytses", "created_at": "2012-09-  
14T14:10:29.000Z", "bio": "", "location": "", "public_email": "", "skype": "", "linkedin": "", "twitter": "sytses", "website_url": "", "organization":  
null, "job_title": "", "pronouns": null, "bot": false, "work_information": null, "followers": 71, "following": 0, "local_time": null }
```

gitlab.com — вывод информации о пользователе

Помимо ссылок на социальные сети, из вывода API Gitlab можно получить зашифрованное значение почты пользователя в параметре avatar\_url. Если мы знаем, например, имя домена и ФИО пользователя, то восстановить исходное значение не составит труда, ведь для хэширования используется md5.

Также в системах контроля версий существуют возможность получения публичных ssh и gpg ключей. Получить их можно по URL-адресам следующего вида:

- <https://github.com/<username>.keys>
- <https://github.com/<username>.gpg>
- <https://bitbucket.org/api/1.0/users/<username>/ssh-keys>
- <https://gitlab.com/<username>.keys>



```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDIuZypOzzT4r+XvjUkHIGMDPmCqkHmJokW73OyNsstUwrhvYZqrsMDdHbD590S1M4pB01JgU/7hesjiRtx2Q  
1H+Ln2Gp5O5+BUcR9dI7ggeLOyzqSb7c76hB3pdZRAuH9IRdEmvzqfZDITN17VQtZzRUjDhradjZ  
/Alc5YGCYYPToCiS4MilGbgqTXydGxEgVubRyWAEa0GxeSvHoNHWS  
/F/4Cen5QUyzzwIyk6xiTPYeA9f+np0tYXn6SAzR0muJqJ4MDeen36dLyunYqUg4INe13PdAAfYDYTM7LDSUezUCyh3UW3iV3zwJd7QNV7i10xRZn  
H2sEhHcxsi36Phh
```

gitlab.com — вывод информации о ключах шифрования пользователя

## Subdomain enumeration

Subdomain enumeration — в дословном переводе означает перечисление поддоменов, а смысл у словосочетания примерно следующий: «использовать все известные методы для получения как можно большего числа поддоменов».



# Coded By Ahmed Aboul-Ela - @aboul3la

```
[~] Enumerating subdomains now for yandex.ru
[~] Searching now in Baidu..
[~] Searching now in Yahoo..
[~] Searching now in Google..
[~] Searching now in Bing..
[~] Searching now in Ask..
[~] Searching now in Netcraft..
[~] Searching now in DNSdumpster..
[~] Searching now in Virustotal..
[~] Searching now in ThreatCrowd..
[~] Searching now in SSL Certificates..
[~] Searching now in PassiveDNS..
```

Запуск утилиты subfinder для поиска поддоменов для доменного имени yandex.ru

Для получения списка поддоменов существуют онлайн базы, а также утилиты, которые требуется запускать локально, после чего они будут делать запросы в различные онлайн сервисы и поисковые системы.

Неполный список сервисов и утилит, которые могут показать список поддоменов для домена:

Online сервисы:

<https://hackertarget.com/find-dns-host-records/>

► Пример результата работы веб-приложения

<https://securitytrails.com/>

► Пример результата работы веб-приложения

<https://cloudflare.com>

► Как получить поддомены с помощью Cloudflare

<https://dnscmdumpster.com/>

По имени домена утилита выводит поддомены, IP-адреса, MX и TXT записи, открытые порты и версии программного обеспечения, DNS-серверы. Также утилита строит красивый граф.

- ▶ Пример результата работы веб-приложения

<https://www.threatminer.org/>

- ▶ Пример результата работы веб-приложения

<https://spyse.com/tools/subdomain-finder>

- ▶ Пример результата работы веб-приложения

Selfhosted:

<https://github.com/about3la/Sublist3r>

Утилита для поиска поддоменов в открытых источниках. Также может перебирать поддомены по словарю, с помощью утилиты subbrute.

- ▶ Пример запуска и результат выполнения утилиты

<https://github.com/projectdiscovery/subfinder>

Очередная утилита для пассивного поиска поддоменов.

- ▶ Пример запуска и результат выполнения утилиты

<https://github.com/OWASP/Amass>

Утилита, как и Sublist3r, ищет информацию о доменах в открытых источниках. Однако, использует гораздо большее число источников, в том числе требующие API-ключи.

- ▶ Пример запуска и результат выполнения утилиты

<https://github.com/blechschmidt/massdns>

Очень быстрая утилита для резолва доменов с достаточно большим количеством ошибок. Позволяет разрезолвить миллион доменных имен за минуту.

- ▶ Пример запуска и результат выполнения утилиты

<https://github.com/projectdiscovery/shuffledns>

Обертка для massdns. Его преимущество заключается в том, что данная утилита удаляет из вывода поддомены, если слишком большое количество доменов указывает на один IP-адрес, тем самым повышая качество вывода.

► Пример запуска и результат выполнения утилиты

Подробнее, об указанных выше утилитах, а также десятках других утилит, можно прочитать в статье: <https://pentester.land/cheatsheets/2018/11/14/subdomains-enumeration-cheatsheet.html>.

## SSL/TLS сертификаты

### Получение новых поддоменов из сертификатов

Для шифрования трафика у веб-приложения должен быть сертификат, по которому браузер пользователя сможет определить, что этот сайт надежен.

Google решил, что протокол https недостаточно надежный, и создал свой проект по мониторингу и проверке сертификатов

<https://transparencyreport.google.com/https/certificates>

Этот сервис предназначен не для тестирования на проникновение или разведки, но так как сертификаты выпускаются как для доменов, так и для поддоменов, а иногда один сертификат даже включает в себя множество доменов и поддоменов, сервис Google может дать нам довольно много информации.

Домен	Издатель	Кол-во имен DNS	Дата начала действия	Дата окончания действия
api.yandex.ru	Yandex CA	22	3 сент. 2020 г.	4 мар. 2021 г.
api.tech.yandex.ru	Yandex CA	49	1 окт. 2019 г.	30 сент. 2020 г.
api.yandex.ru	Yandex CA	22	3 сент. 2020 г.	4 мар. 2021 г.
academy.yandex.ru	Yandex CA	1	30 сент. 2020 г.	22 мар. 2021 г.

transparencyreport.google.com — поиск сертификатов для доменного имени yandex.ru и его поддоменов

Также есть еще как минимум два онлайн сервиса с подобной функциональностью:



<https://spyse.com/tools/ssl-lookup>

- ▶ Пример результата работы веб-приложения

<https://crt.sh/>

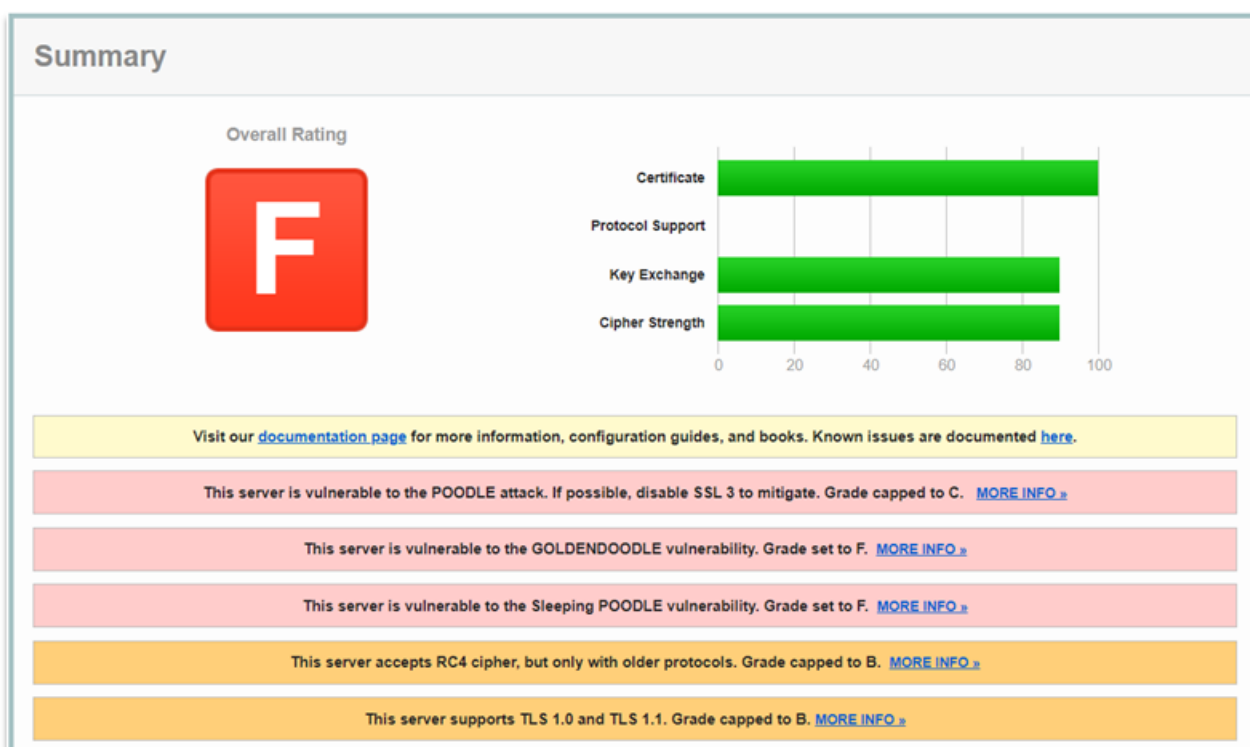
- ▶ Пример результата работы веб-приложения

Существует один self-hosted сервис <https://github.com/lanrat/certgraph>.

- ▶ Пример запуска и результат выполнения утилиты

## SSL/TLS scan

Сертификаты также можно провалидировать. Для этого есть онлайн сервисы, которые за нас отправляют запросы на серверы нашей цели.



ssllabs.com — анализ конфигурации SSL/TLS веб-серверов

Из вывода этих сервисов мы можем опять же получить поддомены, которые есть в сертификате, а также эти сервисы могут найти уязвимости в используемой криптографии или протоколах.

Еще эти сервисы выводят http-ответы серверов, в которых может находиться версия сервера или используемого ПО.

Неполный список сервисов, которые могут просканировать сертификаты.

<https://www.cyphercraft.io/tls>

- ▶ Пример результата работы веб-приложения

<https://ssltools.digicert.com/checker/views/checkInstallation.jsp>

► Пример результата работы веб-приложения

<https://decoder.link/sslchecker>

► Пример результата работы веб-приложения

<https://www.immuniweb.com/ssl/>

► Пример результата работы веб-приложения

<https://www.ssllabs.com/ssltest>

► Пример результата работы веб-приложения

### Что это нам дает?

- Новые поддомены
- Уязвимости криптографии
- Версия используемого ПО на сервере

## Credentials stuffing

---

Credentials stuffing — это атака, при которой атакующий находит почты пользователей и ищет пароли от них в базах утечек, а затем пытается вставить их во все возможные формы входа целевой системы.

Сама атака уже не относится к пассивной разведке, но сбор паролей и email-адресов - это тема данной статьи.

Пароли можно поискать в следующих сервисах:

<https://haveibeenpwned.com/> — самый популярный сервис поиска утечек email-адресов.

► Пример результата работы веб-приложения

- <https://krevetk0.medium.com/credential-stuffing-in-bug-bounty-hunting-7168dc1d3153> — статья исследователя, в которой он рассказывает, как он неоднократно эксплуатировал данную уязвимость в bugbounty.
- <https://psbdmp.cc/> — сервис, который автоматически находит строки, похожие на пароли в файлах, размещенных на веб-сайте [pastebin.com](https://pastebin.com)

► Пример результата работы веб-приложения

- Collection #1 — сборник практически всех утечек, которые попадали в интернет.

- ~~Глазбога.рф~~

## Поиск email-адресов

---

Для проведения атак credential stuffing для социальной инженерии и других атак, необходимо иметь список email-адресов и/или юзернеймов пользователей. Также по email-адресам можно делать поиск reverse Whois.

Нам известно два сервиса, которые собирают email-адреса:

<https://hunter.io/search> — помимо адресов, показывает еще и страницы, где он их нашел.

- ▶ Пример результата работы веб-приложения

<https://snov.io/>

- ▶ Пример результата работы веб-приложения

Также, существует утилита, позволяющая провалидировать почтовые адреса <https://github.com/reacherhq/check-if-email-exists>. Причем она работает без отправки писем на адреса цели. Можно не хостить ее у себя, а воспользоваться веб-версией от разработчиков, с ограничением на количество запросов <https://reacher.email/>.

- ▶ Пример общения с веб-версией

Email-адреса также можно получать из метаданных файлов и парсить из социальных сетей.

## Linkedin\hh.ru\career

---

На сайтах типа linkedin и hh, а также на сайтах компаний, на эндпоинтах \career или \job, можно найти вакансии, в которых зачастую присутствует полезная информация.

В своих резюме и на LinkedIn, пользователи часто указывают кем и где они работают, и часто в описаниях своей работы пишут, чем они конкретно занимаются, например, "поднимал почтовый сервер под названием таким-то", или пишут, что они "переписывали легаси-код с такой-то платформы, но не успели за время своей работы".

Существуют специализированные парсеры соцсетей, например для LinkedIn есть минимум 2 парсера:

<https://github.com/vysecurity/LinkedInt>

- ▶ Пример запуска и результат выполнения утилиты

[https://github.com/joeyism/linkedin\\_scraper](https://github.com/joeyism/linkedin_scraper) — библиотека на python для продвинутых пользователей, для упрощения парсинга linkedin.

Используя эти сервисы, можно получить фамилии и имена сотрудников с их аватарами. По аватарам можно найти другие соцсети сотрудников и попробовать найти что-то полезное, но поиск людей, это тематика для другой статьи.

Если мы знаем формат почты (например имя.фамилия@домен или первая\_буква\_имени.фамилия@домен), то мы можем из полученных ранее данных составить список почт сотрудников.

### Что нам это дает?

- Email-адреса
- Стеки технологий и используемое ПО
- Никнеймы сотрудников
- Информация о сотрудниках для соц. инженерии
- Личные соцсети сотрудников

## Misc

---

В данном разделе собраны подходы, которые не удалось объединить более общими тематиками.

## Co-hosting

---

Анализ co-hosting-а позволяет смотреть кто хостится у этих же провайдеров. Это не принесет полезной информации, если хостинг является, например, hostinger или digital ocean, однако, если компания достаточно большая, у которой есть свои подсети и AS, то мы можем найти доменные имена, расположенные в этих подсетях, которые с большой вероятностью относятся к нашей цели.

Для этого можно воспользоваться сервисом <https://securitytrails.com/>.

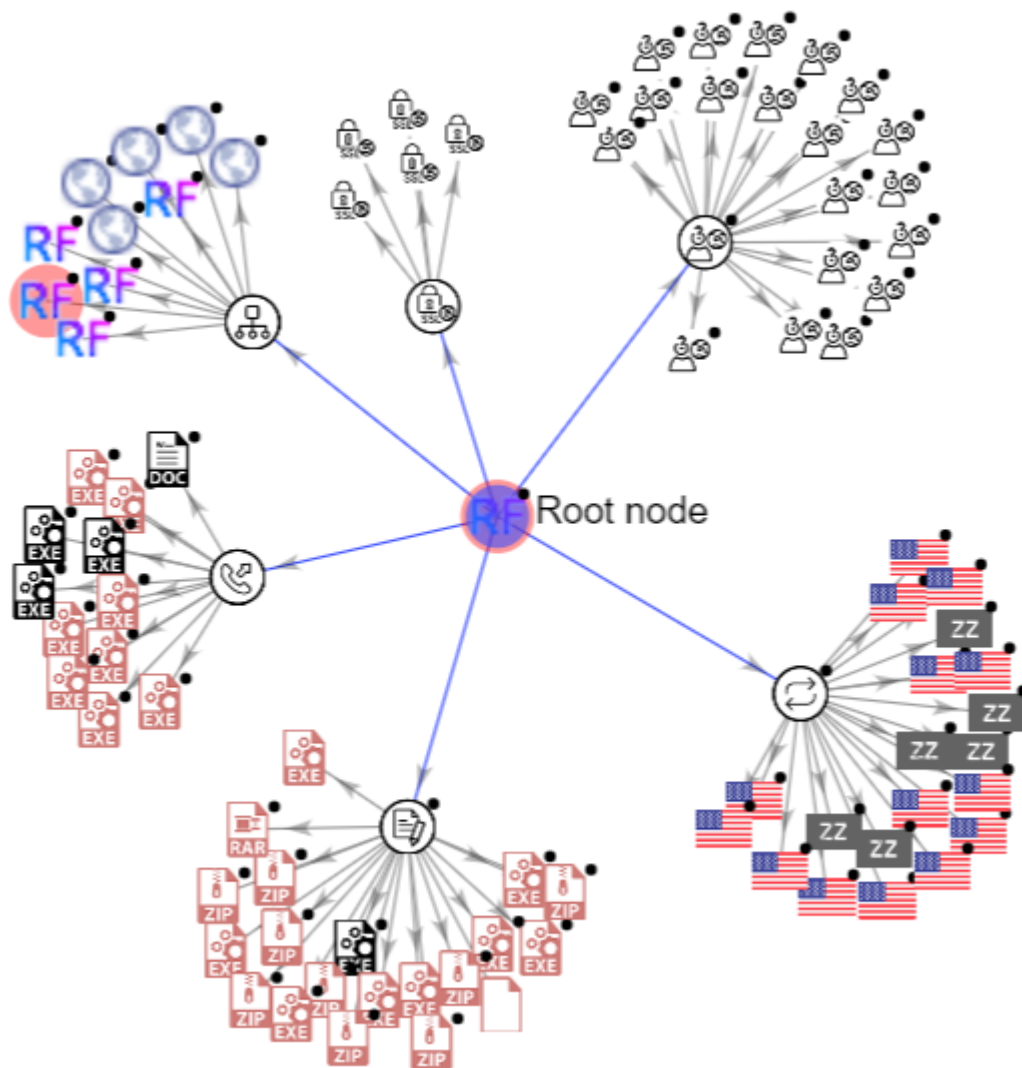
► Пример результата работы веб-приложения

Из этой информации мы можем получить новые поддомены и домены.

## Threat Hunting

---

Вы наверняка знаете что есть сервис [VirusTotal](#), в который можно загрузить подозрительный сэмпл файл и он проверит его на наличие в базах антивирусного ПО, а также можно ему передать ссылку и он также проверит ее на вредоносность. Нам для разведки интересно то, что он еще умеет проверять доменные имена по базам.



virustotal.com — информация о доменном имени raidforums.com в виде графа

На примере домена [raidforums.com](https://raidforums.com), VirusTotal показал множество файлов, которые кто-то загружал для проверки, несколько поддоменов, вывел содержимое Whois, показал IP-адреса и сертификаты. И еще построил граф.

К сожалению, в бесплатной версии мы не можем скачать файлы, которые были загружены в сервис, но это может дать нам подсказку, что можно искать в Google.

Существует несколько сервисов с аналогичной функциональностью, например <https://www.threatcrowd.org/>. Он может все тоже самое, что и VirusTotal, но у них могут быть разные сведения о доменах.

У этих сервисов также есть платные функции, возможно с их помощью можно получить еще больше информации.

## Wayback machine

Wayback machine — проект по сохранению всего интернета, который периодически делает снимки популярных сайтов.



archive.org — веб-приложение, расположенное на доменном имени yandex.ru в 1998 году

Помимо того что можно посмотреть как выглядели сайты в прошлом, и ~~поискать флаги в CTF-соревнованиях~~, также можно найти, например, снапшот критичных файлов, которые администраторы уже удалили, либо снапшот веб-приложения, в коде страницы которого была оставлена какая-нибудь полезная информация для атакующего. Также в снапшотах можно увидеть ошибки и стектрейсы приложений, которые могут помочь развить атаку.

Существует утилита, которая извлекает URL-адреса, сохраненные в Wayback Machine: <https://github.com/tomnomnom/waybackurls>.

```
root@DESKTOP-5MMIEVF:/# echo "test.ru" | waybackurls
http://test.ru
http://test.ru/images/blendbar.jpg
http://test.ru/images/glogo.jpg
http://test.ru/images/glogo2.png
http://test.ru/images/go-button-gateway.gif
http://test.ru/images/petabox-header.png
http://test.ru/robots.txt
http://test.ru/static/images/toolbar/transp-black-pixel.png
http://test.ru/stylesheets/archive.css?v=51519
http://abakan.test.ru
http://adler.test.ru
http://administry.test.ru
http://bugulma.test.ru
http://bugulma.test.ru/robots.txt
http://test,eccon.ru/robots.txt
http://egerus.test.ru/robots.txt
http://ekaterinburg.test.ru
http://expo.test.ru
http://kazan.test.ru
http://msn.test.ru/robots.txt
http://novosibirsk.test.ru
http://pskov.test.ru
http://www.rus.test.ru/robots.txt
http://sitec.test.ru
http://sitec.test.ru/images/blendbar.jpg
http://sitec.test.ru/images/glogo.jpg
http://sitec.test.ru/images/glogo2.png
http://sitec.test.ru/images/go-button-gateway.gif
http://sitec.test.ru/images/petabox-header.png
http://sitec.test.ru/stylesheets/archive.css?v=51519
http://spb.test.ru
http://spb.test.ru/robots.txt
http://ufa.test.ru
http://voronezh.test.ru
```

Поиск URL-адресов в сервисе waybackmachine для доменного имени test.ru с помощью утилиты waybackurls

## Тендеры и закупки

---

При публикации тендеров, заказчики прикладывают к заявке технические задания с описанием требований к исполнителям. Из технического задания можно получить дополнительную информацию о используемом в компании ПО и оборудовании.

Также можно извлечь метаданные из приложенных файлов и получить ФИО сотрудников и версию ПО для обработки документов.



## Тендер: Выполнение работ по внедрению, доработке и поддержке CMS Bloomreach

№43028835

Дата размещения: 28.12.19



Предмет тендера	Выполнение работ по внедрению, доработке и поддержке CMS Bloomreach	Завершён
Начальная цена	12 000 000 рублей	Отрасль
Место поставки	Город Москва	
Организатор закупки	ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ НЕБАНКОВСКАЯ КРЕДИТНАЯ ОРГАНИЗАЦИЯ "ЯНДЕКС.ДЕНЬГИ"	
Окончание приёма заявок	20.01.2020 в 00:00 (МСК) Прием заявок завершён	
Способ размещения	Конкурсы и аукционы	Регион закупки
Ссылки на источники	<a href="#">223-ФЗ ЕИС</a>	

Пример тендерной закупки компании Яндекс.Деньги

## Website fingerprinting

Используя специальные сервисы, не заходя на целевой веб-сайт, мы можем посмотреть версии ПО которые там используются, а также CMS системы, на которых работает веб-сайт, если они есть.

Для этого можно воспользоваться следующими сервисами:

<https://www.wappalyzer.com/>

► Пример результата работы веб-приложения

<https://whatcms.org/>

► Пример результата работы веб-приложения

Такие сервисы парсят заголовки HTTP-ответов, чтобы получать версии ПО, а также смотрят на содержимое страниц для профилирования.

## BugBounty

Далеко не все компании имеют публичную платформу вознаграждений за поиск ошибок, но для больших и крупных это становится одной из лучших практик ИБ.

### Что мы оттуда можем достать?

Расширить область аудита доменами и поддоменами из раздела Scope.

Изучить сданные отчеты и узнать используемое в компании ПО и примеры уязвимостей, которые уже сдавали в программу.

## Где искать информацию?

Платформы BugBounty:

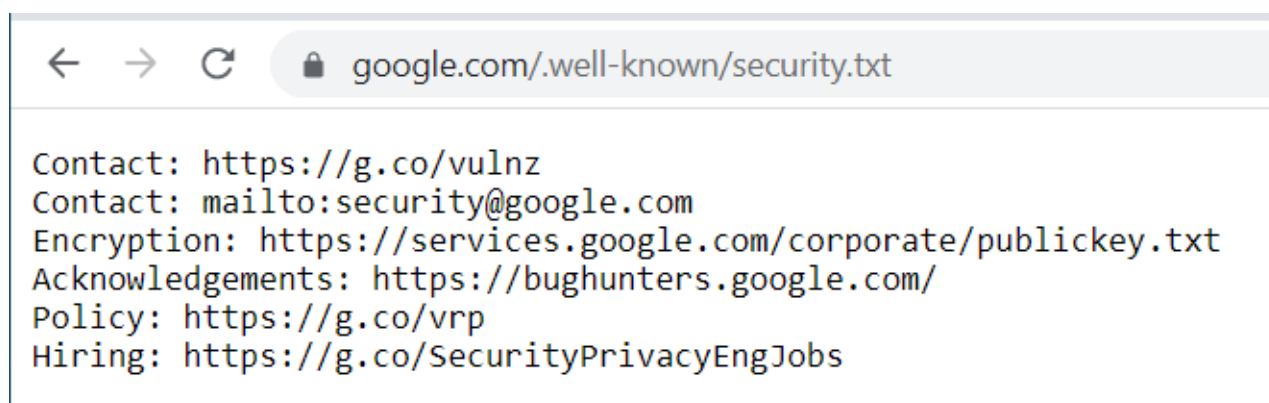
<https://hackerone.com/>

- ▶ Пример результата работы веб-приложения

<https://www.openbugbounty.org/>

- ▶ Пример результата работы веб-приложения

Информацию о BugBounty конкретной организации также можно найти по в файле `/.well-known/security.txt`, в котором обычно публикуется информация о программе и том куда можно писать о найденных уязвимостях. Подробнее о проекте можно прочитать по ссылке <https://securitytxt.org/>.



Пример содержимого файла security.txt

Также существует веб-приложение, которое агрегирует уязвимости с HackerOne, с удобным поиском и фильтрами: <http://h1.nobbd.de/>.

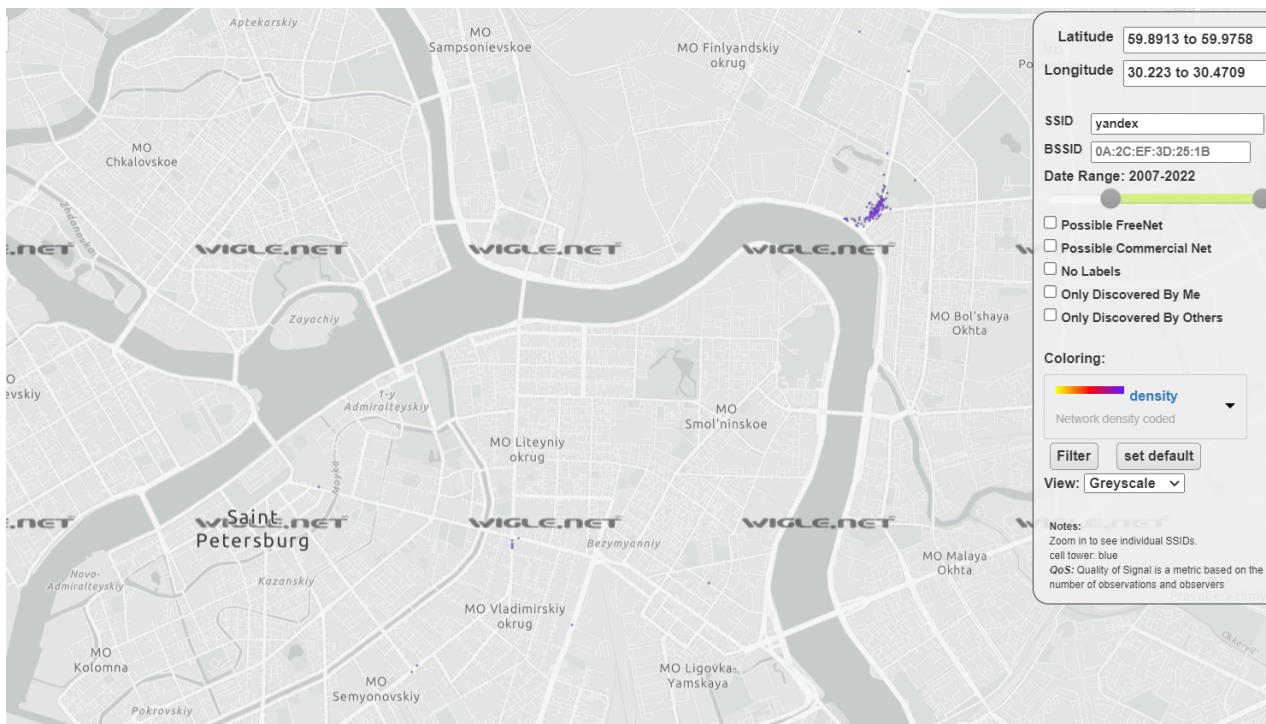


h1.nobbd.de — поиск публичных отчетов по запросу mail.ru

## Wi-Fi анализ

<https://wigo.net/> — сервис, который собирает Wi-Fi точки доступа по всему миру.

Сервис не позволяет просто на карте кликать на точки доступа, однако он позволяет искать по, например, SSID (имя точки доступа). А также он поддерживает регулярные выражения: "%" — ноль или более любых символов и "\_" — один любой символ.



Поиск точек доступа Wi-Fi с именем yandex в сервисе wigo.net

Эту информацию можно использовать для атак типа Rogue access point и атак социальной инженерии.

## MAC address lookup

В рамках пассивной разведки, маловероятно, что вы получите MAC-адреса устройств вашей цели. Однако, если вам как-то удалось их заполучить, то имея только MAC-адрес можно идентифицировать сетевое устройство.

### MAC Address Details

Company	Uniclass Technology, Co., LTD
Address	Hsintien City Taipei Hsien 231 TAIWAN, PROVINCE OF CHINA
Range	00:11:AA:00:00:00 - 00:11:AA:FF:FF:FF
Type	IEEE MA-L

macvendorlookup.com — идентификация сетевого устройства по MAC-адресу

MAC-адрес можно разделить на 6 октетов, где первые 3 принадлежат компании-производителю сетевого устройства, а вторые 3 октета являются идентификатором самого устройства.

Используя специальные сервисы и читщиты производителей, можно попробовать узнать не только производителя, но и название самого устройства:

<https://dnschecker.org/mac-lookup.php>

► Пример результата работы веб-приложения

<https://www.macvendorlookup.com>

## Script Kiddie way

---

Искать информацию руками долго и утомительно, зато надежно. Однако хакеры придумали комбайны, которые все сделают за вас. Этим комбайнов десятки, если не сотни, вот несколько примеров:

- <https://github.com/s0md3v/ReconDog>
- [https://github.com/eldraco/domain\\_analyzer](https://github.com/eldraco/domain_analyzer)
- <https://github.com/smicallef/spiderfoot>
- <https://github.com/laramies/theHarvester>
- <https://github.com/j3ssie/Osmedeus>
- <https://www.maltego.com/downloads/>
- <https://github.com/lanmaster53/recon-ng>

### В чем отличие от ручного поиска?

Их преимущество в том, что освобождают человека от рутинных задач.

А недостатки заключаются в следующем:

- Длительная первоначальная конфигурация.
- Длительное время работы.
- Необходимость (желательность) предоставления API-ключей от различных сервисов (балансы которых они быстро опустошат).
- Большое количество ошибок как первого так и второго рода (множество лишней информации и отвергнутая нужная информация)

Если вы знаете еще интересные способы поиска информации в интернете, то пишите об этом в комментариях!

