

Нетсталкинг

Как хакеры и злоумышленники могут найти информацию с помощью Google и дорков



8bit



Wininvestor



CyberYozh Security Group

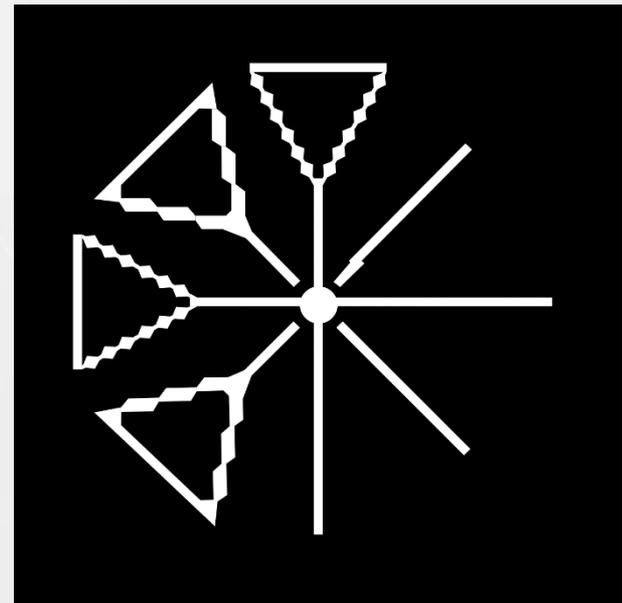


Anti-Malware



Нетсталкинг

Нетсталкинг (англ. *netstalking*) — это деятельность, осуществляемая в пределах сети методом поиска, направленная на обнаружение малоизвестных, малодоступных и малопосещаемых объектов с их возможным последующим анализом, систематизацией и хранением, с целью эстетического и информационного удовлетворения искателя.



Друзья нетсталкера



```

root@kali:~# zoomeye search mikrotik
ip:port          service          country          app              banner
187.162.37.85:8123 http            Mexico          MikroTik router co ... HTTP/1.0 200 OK\r\nConn ...
213.59.200.182:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.238.206:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.153.194:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.239.250:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.193.214:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.239.170:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.219.202:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.193.210:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.194.74:2222  ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.193.230:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.228.230:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.159.219:2222 ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
213.59.136.44:2222  ssh            Russian Federation MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
107.145.24.181:23  ssh            United States   MikroTik RouterOS sshd SSH-2.0-ROSSSH\r\n
45.224.8.15:7171   routeros-api   Argentina      MikroTik RouterOS API  \x06!fatal\r\nnot logged ...
190.92.110.158:7777 http           Argentina      MikroTik router co ... HTTP/1.0 200 OK\r\nConn ...
190.93.220.198:7777 http           Argentina      MikroTik router co ... HTTP/1.0 200 OK\r\nConn ...
54.159.157.184:4000 https         United States   Microsoft IIS httpd   HTTP/1.0 302 Found\r\nD ...
54.154.175.112:4000 https         Ireland         AVM FRITZ!Box        HTTP/1.0 302 Found\r\nD ...

```

total: 20/29622291

Около 34 698 631 результат (Почти год: 11 874 143 результатов) 1,708 секунды

Рейтинг ценности

микротик X

18.144.34.250 >

8884 / http

IDC

США, Сан-Франциско

2021-09-14 16:19

Amazon.com, Inc.

amazon.com

ASN: AS16509

Баннер Файл

HTTP / 1.0 302 Найдено

Дата: вторник, 14 сентября 2021 г., 08:19:06 GMT

X-Powered-By: PHP / 5.4.45

48 (Mandrake Linux / 6.8.100mdk) mod_perl / 1.99_11 Perl / v5.8.3 mod_ssl

Расположение: http://125.64.94.144:8884/

Content-Length: 0



ТИП ПОИСКА

Устройства	34 574 027 ▼
IPv4	34 559 577
IPv6	14 450
Сайты	124 609

Dorks

- site — поиск по конкретному сайту;
- inurl — указатель на то, что искомые слова должны быть частью самого веб-адреса;
- intitle — оператор поиска в заголовке веб-страниц;
- ext или filetype — поиск файлов определенного типа по расширению.
- Также при составлении запроса надо помнить несколько операторов, которые задаются спецсимволами.
- | — вертикальный слеш, он же оператор OR (логическое или).
Указывает, что нужно показать результаты, содержащие хотя бы одно из слов, перечисленных в запросе.
- "" кавычки. Указывает на поиск точного соответствия.





Jira Software

Уязвимые URL

`/secure/popups/UserPickerBrowser.jspa`

`/secure/ManageFilters.jspa?filterView=popular`

`/secure/ConfigurePortalPages!default.jspa?view=popular`

Пример запроса

`Inurl:/secure/ManageFilters.jspa?filterView=popular`



Результатов: примерно 2 900 (0,49 сек.)

<https://community.atlassian.com> > ... ▾ Перевести эту страницу

Solved: /jira/secure/ManageFilters.jspa?filterView=search

10 сент. 2018 г. — Solved: Hello everyone, i need some guidance on how to turn this **filter view** off for not log in users? Also is there some type of jira ...

Не найдено: ~~xxxx~~ | Запрос должен включать: **Inurl**

Вы посещали эту страницу 28.07.21.

<https://jira.atlassian.com> > JRA... ▾ Перевести эту страницу

Anonymous user is unable to access Manage Dashboard ...

The user needs to manually navigate to the **URL** to access this page. Notes. This applies to <Base **URL**>/secure/ManageFilters.jspa?filterView=popular as well ...

Вы посещали эту страницу несколько раз (2). Дата последнего посещения: 28.07.21

<https://at.projects.genivi.org> > ... ▾ Перевести эту страницу

Manage Filters - Jira

Filters are issue searches that have been saved for re-use. This page shows you the most **popular** filters. Name, Shared With, Subscriptions, **Popularity** ...

Не найдено: ~~xxxx~~ | Запрос должен включать: **Inurl**

Вы посещали эту страницу несколько раз (3). Дата последнего посещения: 28.07.21

<https://www.exasol.com> > secure ▾ Перевести эту страницу

Manage Filters - Issue Tracker - Exasol

Filters are issue searches that have been saved for re-use. This page shows you the most **popular** filters. Name, Shared With, Subscriptions, **Popularity** ...

Не найдено: ~~xxxx~~ | Запрос должен включать: **Inurl**



Moodle Tracker

Дашборды ▾

Проекты ▾

Проблемы ▾

Захватывать ▾



Авторизоваться

Просмотр проектов

ТИПЫ ПРОЕКТОВ

Все типы проектов

Программное обеспечение

Бизнес

Все типы проектов - Все категории

Проект ↑	Ключ	Тип проекта	Руководитель проекта	Категория проекта	URL
Moodle	Лей		Сандер Бангма	Нет категории	http://moodle.org/
Приложен...	МОБИЛЬНЫЙ		Хуан Лейва	Нет категории	http://docs.moodle.
Сайты соо...	MDLSITE		Хелен Фостер	Нет категории	http://moodle.org/
Moodle QA	MDLQA		moodle.com	Нет категории	https://docs.moodle
MoodleNet	MDLNET		Пол Ходжсон	Нет категории	https://moodle.net
Плагины	ВНОСИТЬ		Дэвид Мудрак (@ r	Нет категории	https://moodle.org/

Open issues Switch filter ▾

[View all issues and filters](#)

Order by Priority ▾ 

 [CODETOOLS-7900033](#)
need better logging and error report...

 [CODETOOLS-7901836](#)
Cannot get VM for test during run ja...

 [CODETOOLS-7901445](#)
JVM crash or assert during System....

 [CODETOOLS-7902162](#)
4 compiler/jvnci tests fail when run...

 [CODETOOLS-7900887](#)
ChoiceArrayQ doesn't allow disabli...

 [CODETOOLS-7902347](#)
There are no test result and test arti...

 [CODETOOLS-7902067](#)
CachingTestFilter caches based on ...

 [CODETOOLS-7902032](#)
jtreg does not merge platforms from...

 [CODETOOLS-7901922](#)
Introduce builder API for Jcov file o...

 [CODETOOLS-7902078](#)
Create a README file for Jemmy v3.

 [CODETOOLS-7902033](#)
Provide open-source test support

 [CODETOOLS-7901991](#)
Extend Jcov report with "non-cover...



[Code Tools](#) / [CODETOOLS-7902032](#)

8 of 516   

jtreg does not merge platforms from multiple exclude files

 Export ▾

Details

Type:  Bug
 Status: **NEW**
 Priority:  P2
 Resolution: Unresolved
 Affects Version/s: None
 Fix Version/s: None
 Component/s: [tools](#)
 Labels: None
 Subcomponent: [jtreg](#)

Description

Some tests cannot run successfully in our testing infrastructure so we added a closed/ProblemList.txt to exclude these.

One example is:

```
$ ack NoLoopbackPackets ProblemList.txt closed/ProblemList.txt
ProblemList.txt
166:java/net/MulticastSocket/NoLoopbackPackets.java 7122846 macosx-all

closed/ProblemList.txt
5:java/net/MulticastSocket/NoLoopbackPackets.java
```

As you can see we want to exclude the test on all platforms but it doesn't work.

People

Assignee:  Unassigned
 Reporter:  [Christian Thalinger](#)
 Votes:  0 Vote for this issue
 Watchers:  2 Start watching this issue

Dates

Created: 2017-09-15 11:09
 Updated: 2018-05-02 12:58



Редактировать текущий фильтр ?

Название*

Описание

Избранный

Читатели Не использовать совместно

Добавить читателей

+ Добавить



Trello

Trello — ещё один проект от Atlassian. Это один из самых известных таскменеджеров. Им успешно пользуются не только компании, но и обычные люди (в качестве записной книжки или средства планирования дня)

Изменение видимости ✕

 **Приватная** ✓

Просматривать и изменять эту доску могут только добавленные на нее участники.

 **Рабочее пространство**

Просматривать и изменять эту доску могут все участники рабочего пространства «рабочее пространство».

 **Организация**

Просматривать эту доску могут все сотрудники организации. Чтобы предоставить это разрешение, доску нужно добавить в корпоративное рабочее пространство.

 **Публичная**

Просматривать эту доску могут все в Интернете (в том числе поисковые роботы Google). Изменять ее могут только участники.



билайн симкарта [redacted] Вконтакте [redacted] пароль: [redacted] ✕

[redacted] а

в колонке соц сети

☰ Описание

☰ Действия

Показать подробности

ДЕЙСТВИЯ

📄 Копирование

👤 Подписаться

🔗 Поделиться

соц сети

вк Анна 89537888598 ghbdtn123
навсегда

билайн симкарта 89658212335
Вконтакте Арина булочкина
пароль: boss1243 навсегда

БОООТ НАСТИ МОРОЗОВА ЧАТ
ПЛЮС ВСЕЧтобы видеть кто
проголосовал нужно
проголосовать сначала самому вот
опросник https://vk.com/wall-181622481_129 Новый РК, в нем
нужно пополнить бюджет с карты
на 1000 р. Морозова Настя логин
69236360516 пароль: [redacted] 5

Билайн симкарта 9658212383
ВКОНТАКТЕ [redacted] пароль: [redacted]

Тамара Сова логин 89:
пароль [redacted]

вк страничка ВИКТОРИЯ
ИВАННИКОВА 69930015252
Trade@2019

8 Пароль: [redacted]

вк страничка МАРИЯ [redacted]

2 пароль: [redacted] 4

вк страничка Алиса Котова

89658212335 Пароль: [redacted]

доступ к почте sova5454@mail.ru
и там же biz.mail.ru домен

доступ к домену на per.ru sova54

Зарплата ру: логин

пароль: gh

Антон

...



Паспорт

@ 2

права

медицинский полис

ОБРАЗЕЦ

...

КОНТРАГЕНТ

🕒 1 фев 2020 г.

☰

A

Образец

🕒 1 фев 2020 г.

☰

☑️ доставка оплачена

☑️ Прибыло В ТК города отправки

Какой ТК отправили: Фаворит 56

Кем заказ сформирован: Ирина

мест в ТК: 1 Объем груза: 1,2

Вес: 603

A



Firebase

Google знает, но молчит



site:.firebaseio.com



[Все](#)

[Картинки](#)

[Новости](#)

[Покупки](#)

[Карты](#)

[Ещё](#)

[Настройки](#)

[Инструменты](#)

Результатов: 1 (0,28 сек.)

[Ссылки Google](#)

[Попробуйте Google Search Console](#)

www.google.com/webmasters/

Вы являетесь владельцем **.firebaseio.com**? Получите данные индексирования и рейтинг от Google.

www.firebaseio.com [▼ Перевести эту страницу](#)

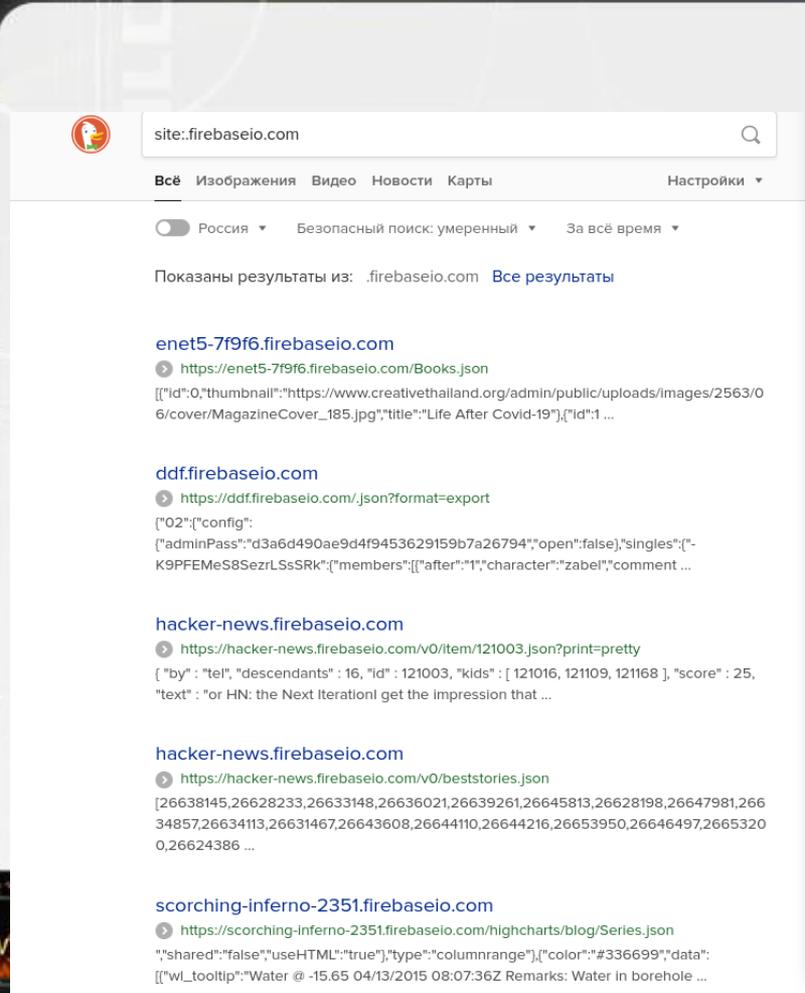
[Firebaseio.com](#)

Информация об этой странице недоступна.

[Подробнее...](#)

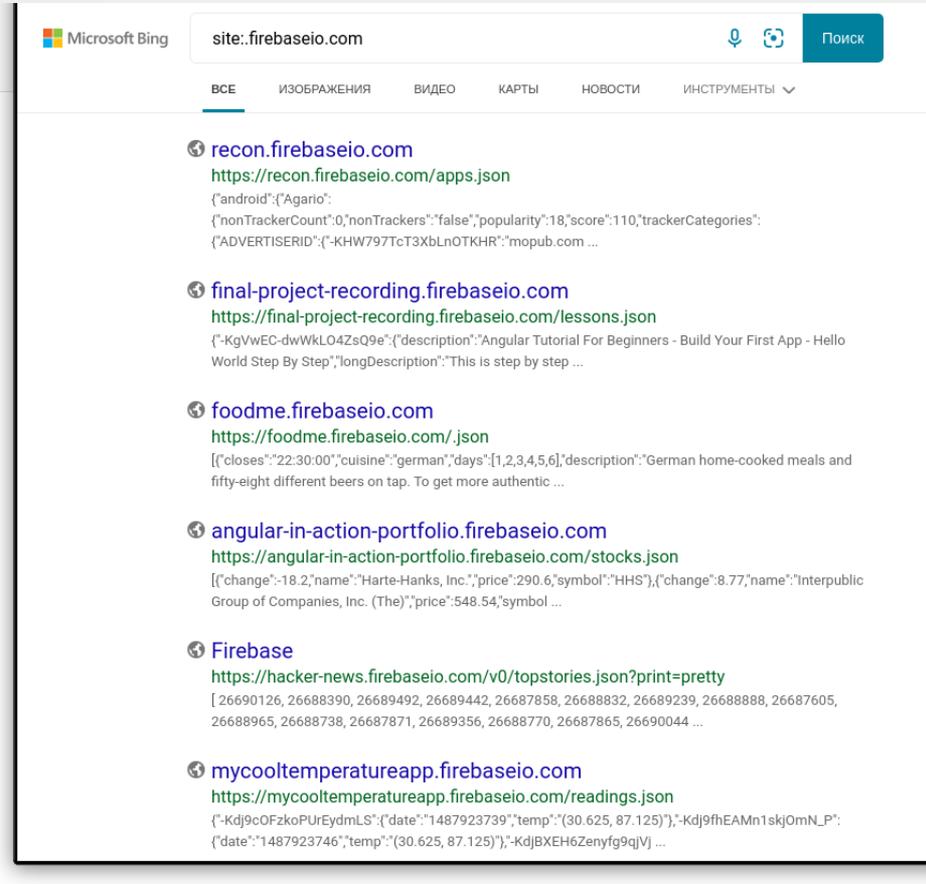


Но вам не спрятаться за его спиной



Search results for `site:firebaseio.com` on a search engine. The results list several domains and their corresponding JSON files:

- enet5-7f9f6.firebaseio.com**
<https://enet5-7f9f6.firebaseio.com/Books.json>
Thumbnail: `[[{"id": "0", "thumbnail": "https://www.creativethalland.org/admin/public/uploads/images/2563/06/cover/MagazineCover_185.jpg", "title": "Life After Covid-19"}], [{"id": "1 ...`
- ddf.firebaseio.com**
<https://ddf.firebaseio.com/.json?format=export>
Snippet: `{"02": {"config": {"adminPass": "d3a6d490ae9d4f9453629159b7a26794", "open": false, "singles": [{"K9PFEMeS8SezrLSsSRK": {"members": [{"after": "1", "character": "zabel", "comment ...`
- hacker-news.firebaseio.com**
<https://hacker-news.firebaseio.com/v0/item/121003.json?print=pretty>
Snippet: `{"by": "tel", "descendants": 16, "id": 121003, "kids": [121016, 121109, 121168], "score": 25, "text": "or HN: the Next Iteration! get the impression that ...`
- hacker-news.firebaseio.com**
<https://hacker-news.firebaseio.com/v0/beststories.json>
Snippet: `[26638145, 26628233, 26633148, 26636021, 26639261, 26645813, 26628198, 26647981, 26634857, 26634113, 26631467, 26643608, 26644110, 26644216, 26653950, 26646497, 26653200, 26624386 ...`
- scorching-inferno-2351.firebaseio.com**
<https://scorching-inferno-2351.firebaseio.com/highcharts/blog/Series.json>
Snippet: `"shared": false, "useHTML": true, "type": "columnrange"}, {"color": "#336699", "data": [{"wl_tooltip": "Water @ -15.65 04/13/2015 08:07:36Z Remarks: Water in borehole ...`



Search results for `site:firebaseio.com` on Microsoft Bing. The results list several domains and their corresponding JSON files:

- recon.firebaseio.com**
<https://recon.firebaseio.com/apps.json>
Snippet: `{"android": {"Agario": {"nonTrackerCount": 0, "nonTrackers": false, "popularity": 18, "score": 110, "trackerCategories": {"ADVERTISERID": {"KHW797TcT3XbLnOTKHR": "mopub.com ...`
- final-project-recording.firebaseio.com**
<https://final-project-recording.firebaseio.com/lessons.json>
Snippet: `{"-KgVwEC-dwWkL04ZsQ9e": {"description": "Angular Tutorial For Beginners - Build Your First App - Hello World Step By Step", "longDescription": "This is step by step ...`
- foodme.firebaseio.com**
<https://foodme.firebaseio.com/.json>
Snippet: `[{"closes": "22:30:00", "cuisine": "german", "days": [1, 2, 3, 4, 5, 6], "description": "German home-cooked meals and fifty-eight different beers on tap. To get more authentic ...`
- angular-in-action-portfolio.firebaseio.com**
<https://angular-in-action-portfolio.firebaseio.com/stocks.json>
Snippet: `[{"change": -18.2, "name": "Harte-Hanks, Inc.", "price": 290.6, "symbol": "HHS"}, {"change": 8.77, "name": "Interpublic Group of Companies, Inc. (The)", "price": 548.54, "symbol": ...`
- Firebase**
<https://hacker-news.firebaseio.com/v0/topstories.json?print=pretty>
Snippet: `[26690126, 26688390, 26689492, 26689442, 26687858, 26688832, 26689239, 26688888, 26687605, 26688965, 26688738, 26687871, 26689356, 26688770, 26687865, 26690044 ...`
- mycooltemperatureapp.firebaseio.com**
<https://mycooltemperatureapp.firebaseio.com/readings.json>
Snippet: `{"-Kdj9cOFzkoPurEydmlS": {"date": "1487923739", "temp": "(30.625, 87.125)"}, {"-Kdj9fHEAMn1skjOmN_P": {"date": "1487923746", "temp": "(30.625, 87.125)"}, {"-KdjBXEH6Zenyfg9qjV ...`

Автоматизируем <https://github.com/Turr0n/firebase.git>

```
Crawling https://sina.firebaseio.com/.json ...
Crawling https://mail.firebaseio.com/.json ...
Crawling https://weibo.firebaseio.com/.json ...
Crawling https://adobe.firebaseio.com/.json ...
Crawling https://reddit.firebaseio.com/.json ...
Crawling https://microsoftonline.firebaseio.com/.json ...
Crawling https://nih.firebaseio.com/.json ...
Crawling https://kompas.firebaseio.com/.json ...
Crawling https://netflix.firebaseio.com/.json ...
Crawling https://babytree.firebaseio.com/.json ...
Crawling https://tribunnews.firebaseio.com/.json ...
Crawling https://bing.firebaseio.com/.json ...
Crawling https://etsy.firebaseio.com/.json ...
Crawling https://onlinesbi.firebaseio.com/.json ...
Crawling https://linkedin.firebaseio.com/.json ...
Crawling https://detik.firebaseio.com/.json ...
Crawling https://17ok.firebaseio.com/.json ...
Crawling https://sohu.firebaseio.com/.json ...
Crawling https://spotify.firebaseio.com/.json ...
Crawling https://bbc.firebaseio.com/.json ...
Crawling https://myshopify.firebaseio.com/.json ...
Crawling https://so.firebaseio.com/.json ...
Crawling https://primevideo.firebaseio.com/.json ...
Crawling https://digikala.firebaseio.com/.json ...
Crawling https://stackexchange.firebaseio.com/.json ...
Crawling https://xvideos.firebaseio.com/.json ...
Crawling https://tmall.firebaseio.com/.json ...
Crawling https://51.firebaseio.com/.json ...
Crawling https://github.firebaseio.com/.json ...
Crawling https://alipay.firebaseio.com/.json ...
Crawling https://tianya.firebaseio.com/.json ...
Crawling https://chaturbate.firebaseio.com/.json ...
Saving results to results.json

404 DBs:          37
Secure DBs:      171
Possible vulnerable DBs: 1
Vulnerable DBs:  25

bit@kali:~/tools/subbrute-master$ python3 subbrute.py firebaseio.com
firebaseio.com
server.firebaseio.com
ulianagv.firebaseio.com
vp.firebaseio.com
vivaesbootlegs.firebaseio.com
mp3track.firebaseio.com
adsense-ja.firebaseio.com
filmesporno.firebaseio.com
foodwishes.firebaseio.com
wijzeman.firebaseio.com
billboard.firebaseio.com
india-paidtoclick.firebaseio.com
sexoffenderissues.firebaseio.com
cultura-del-frumento.firebaseio.com
atdoru.firebaseio.com
falageo.firebaseio.com
underground-kings.firebaseio.com
mspandrew.firebaseio.com
nimblebodhi.firebaseio.com
tricot.firebaseio.com
jarida-tarbawiya.firebaseio.com
simplexworldnews.firebaseio.com
kiminda.firebaseio.com
amalqm.firebaseio.com
seoadmin.firebaseio.com
accounting.firebaseio.com
alpa.firebaseio.com
as76.firebaseio.com
basinger.firebaseio.com
booth10.firebaseio.com
capps.firebaseio.com
chub.firebaseio.com
cp7.firebaseio.com
dcomm1675.firebaseio.com
dietrich.firebaseio.com
duchess.firebaseio.com
```

**И ничего нам за это не будет,
но это не точно**





Telegram:@eightbit