Drive Into the DarkWeb

Jie @ iThome CyberSec 2024

Disclaimer

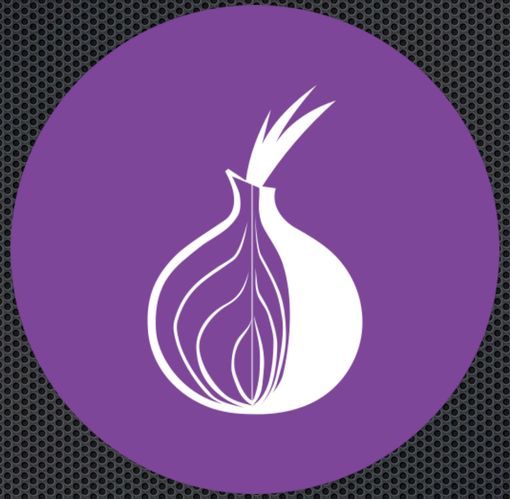
This talk is given by me as an individual
My employer is not involved in any way

whoami

資安說書人

https://www.linkedin.com/in/jieliau
https://github.com/jieliau
https://www.facebook.com/jie.liau
https://twitter.com/0xJieLiau
https://jieliau.medium.com/

DarkWeb



BF

torch

Torch: The Tor Search Engine

Welcome to Jie's nginx!

BF SELL TAIWAN 3G SURVEILLANC

https://breachforums.is/Thread-SELL-TAIWAN-3G-SURVEILLANCE-DATA

Databases | Upgrades | Search | Hidden Service | Extras | Login

BreachForums > Leaks > Other Leaks > SELL TAIWAN 3G SURVEILLANCE DATA

Mark all as re

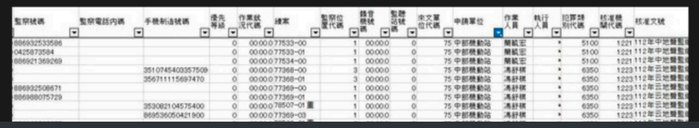
SELL TAIWAN 3G SURVEILLANCE DATA

by fsadoftjy - Tuesday December 5, 2023 at 10:12 AM

fsadoftjy

Yesterday, 10:12 AM

Selling 3g Taiwan surveillance data for 100000USD. contact:fsadoftjy@proton.me



LolzTeam

LVL 3 | 30 Boosts

Browse Channels NEW

lzt.market

zelenka.guru

ВЕРИФИКАЦИЯ

| верификация

ВАЖНОЕ

| правила

| новости

| памятка

| роли

ОБЩЕНИЕ

общение

мемасы

команды

тиммейты

флудилка

ПОДДЕРЖКА / SUPPORT

важно—info

ГОЛОСОВЫЕ КАНАЛЫ

Комната 1

Комната 2

| новости | Follow

Search

Welcome to # | новости!

This is the start of the # | новости channel.

April 27, 2023

miroshi 04/27/2023 4:57 PM

→ **Всем нам иногда хочется немного потоксичить и выплеснуть куда-то накопленные негативные эмоции и агрессию.**

→ *В таком случае, если вы хотите высказаться и выпустить весь пар, который накопился за какое-либо время, то ждём вас на нашем Токсик баттле! На этот раз вы сможете сполна оторваться на других людях, ведь запрещённых слов и фраз не будет, и вы сможете дать волю своей фантазии и отойти от дискордовских шаблонов.*

ПРИЗОВЫЕ МЕСТА:

1. 2500 рублей
2. 1500 рублей
3. 1000 рублей

Время проведения: 30-го апреля — в 20:00 по мск

@here читаем выше новость!

121

May 29, 2023

miroshi 05/29/2023 5:58 PM

Некоторые фиксы завезли.

- Приватки снова работают в штатном режиме.
- Экономика серверу немного пофиксили, пишем другого бота.

20

June 17, 2023

miroshi 06/17/2023 11:02 AM

Удалён канал "селфи"

14:49 73%

Leaks Sh

1144 members, 35 online

Pinned Message

https://

全国车主76万2020年.rar

145.3 MB RAR

car owner china 2020 12:24

tw户籍分割.rar

469.4 MB RAR

Taiwan citizen 12:24

江西移动联通数据库

065万.7z.001

27 GB 001

hina Mobile and

com 12:24

eolpe.rar

18 GB RAR

citizen 12:25

.001

29.2 MB 001

ss 12:25

主.7z.001

00 GB 001

主.7z.002

33 GB 002

use owner 12:25

74

00w机主.7z

t allowed

14:49 73%

APT 28 | Fancy Bear

58 subscribers

Previous Message

iOS Exploit РЦЭ | 0Нажмите | iOS версии 17+ поддержива...

WhatApp Exploit

Поддержка Android и iOS | РЦЭ | 1Нажмите

Контроль над устройством

Дистанционное поддержка

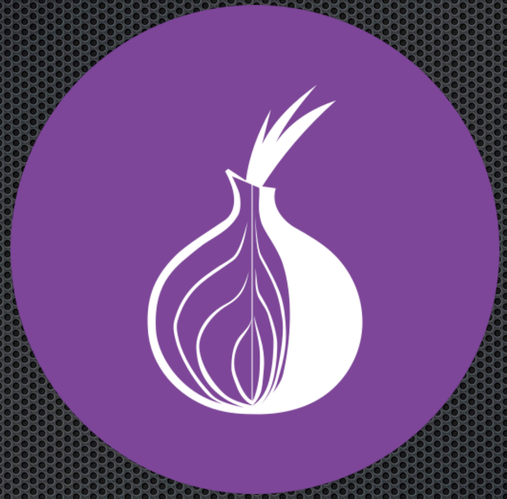
Цена: Торги

КУПИТЬ СЕЙЧАС: @RogachDeveloper

103 edited 02:15

Chrome Exploit

MUTE



The Onion Router

Developed around the mid-1990s by

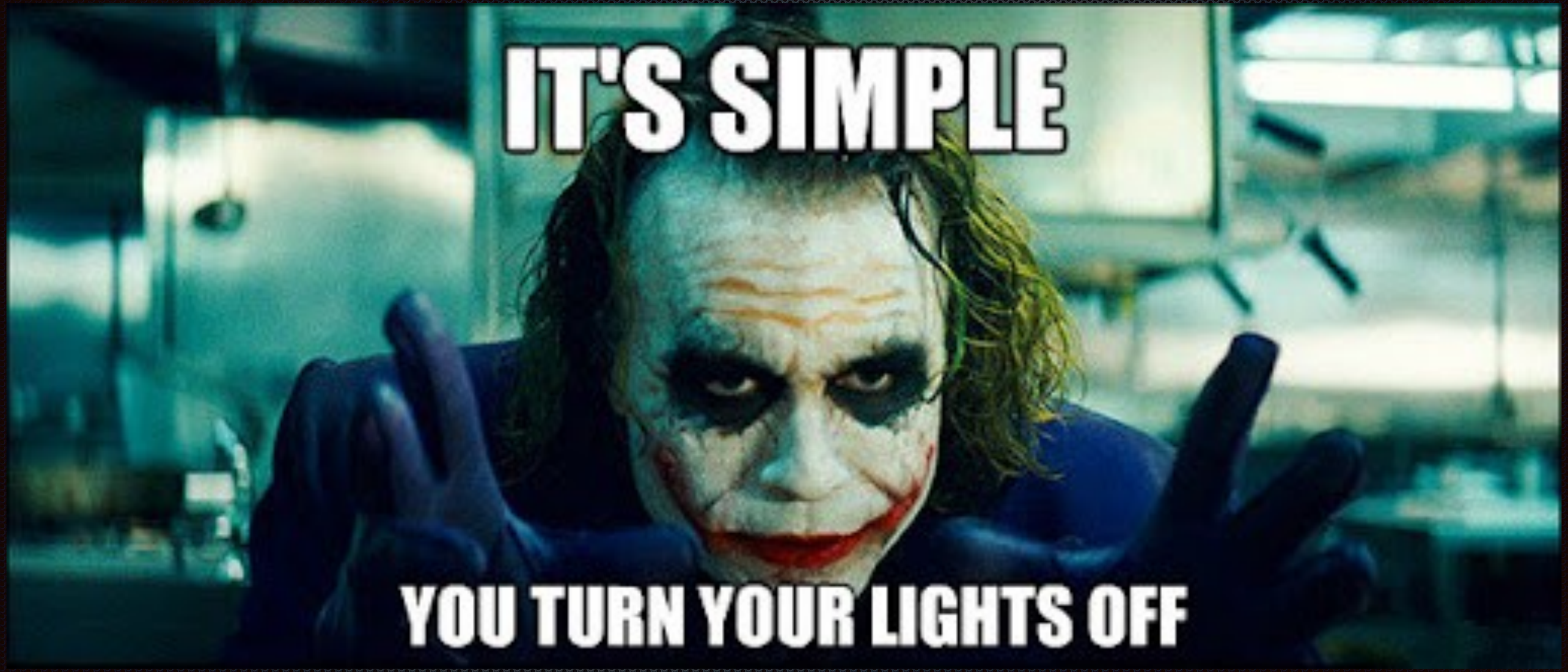
United States Naval Research Laboratory

To protect U.S. intelligence communication online

v2 vs. v3

- http://expyuzz4wqqyqhjn.onion/
  - The hash of the RSA public key
  - 16 characters
- http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion/
  - The full ed25519 public key
  - 56 characters

How to Get on DarkWeb


IT'S SIMPLE
YOU TURN YOUR LIGHTS OFF

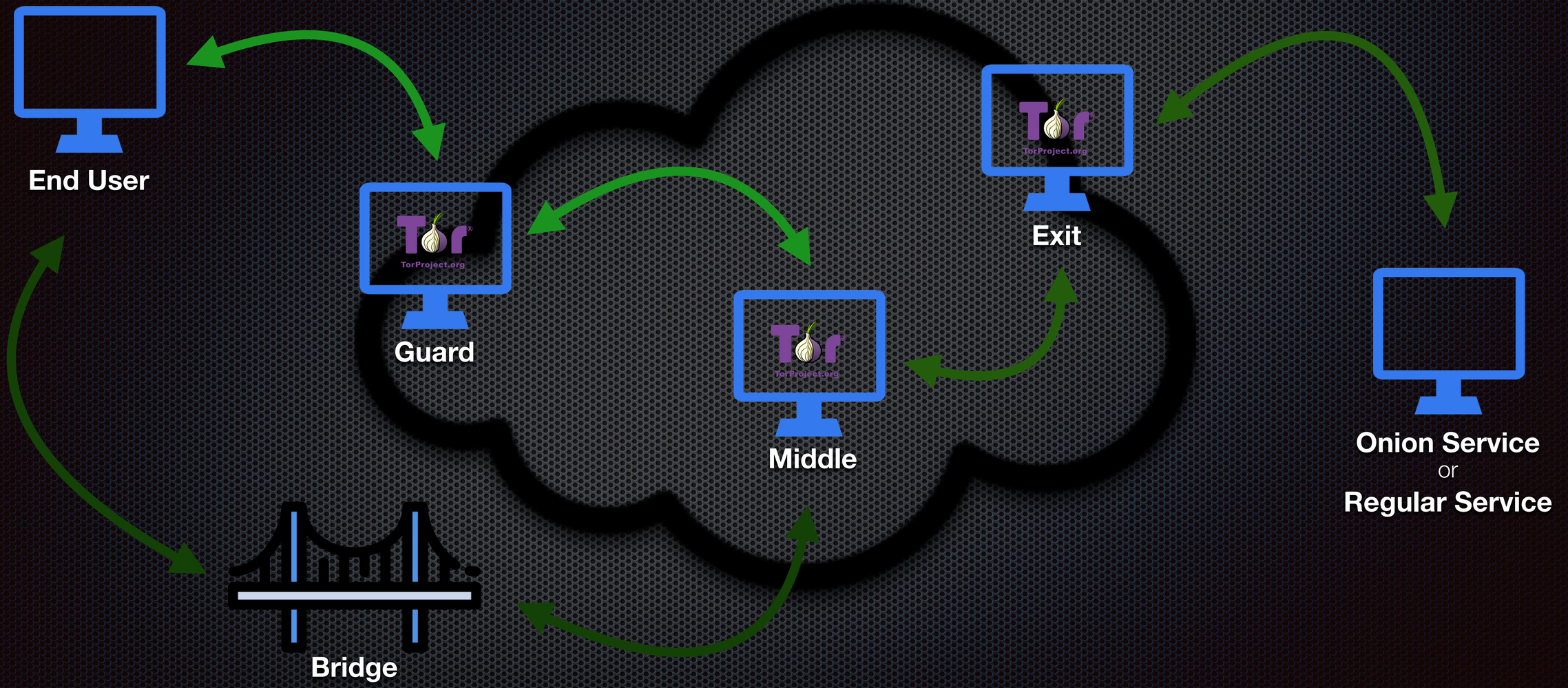
Get On DarkWeb

- **Tor Browser bundle**
  - https://www.torproject.org/download/
- **Whonix**
  - https://www.whonix.org/
- **Tails**
  - https://tails.net/

Node Types

IP addresses of 3 types of Tor relay are public

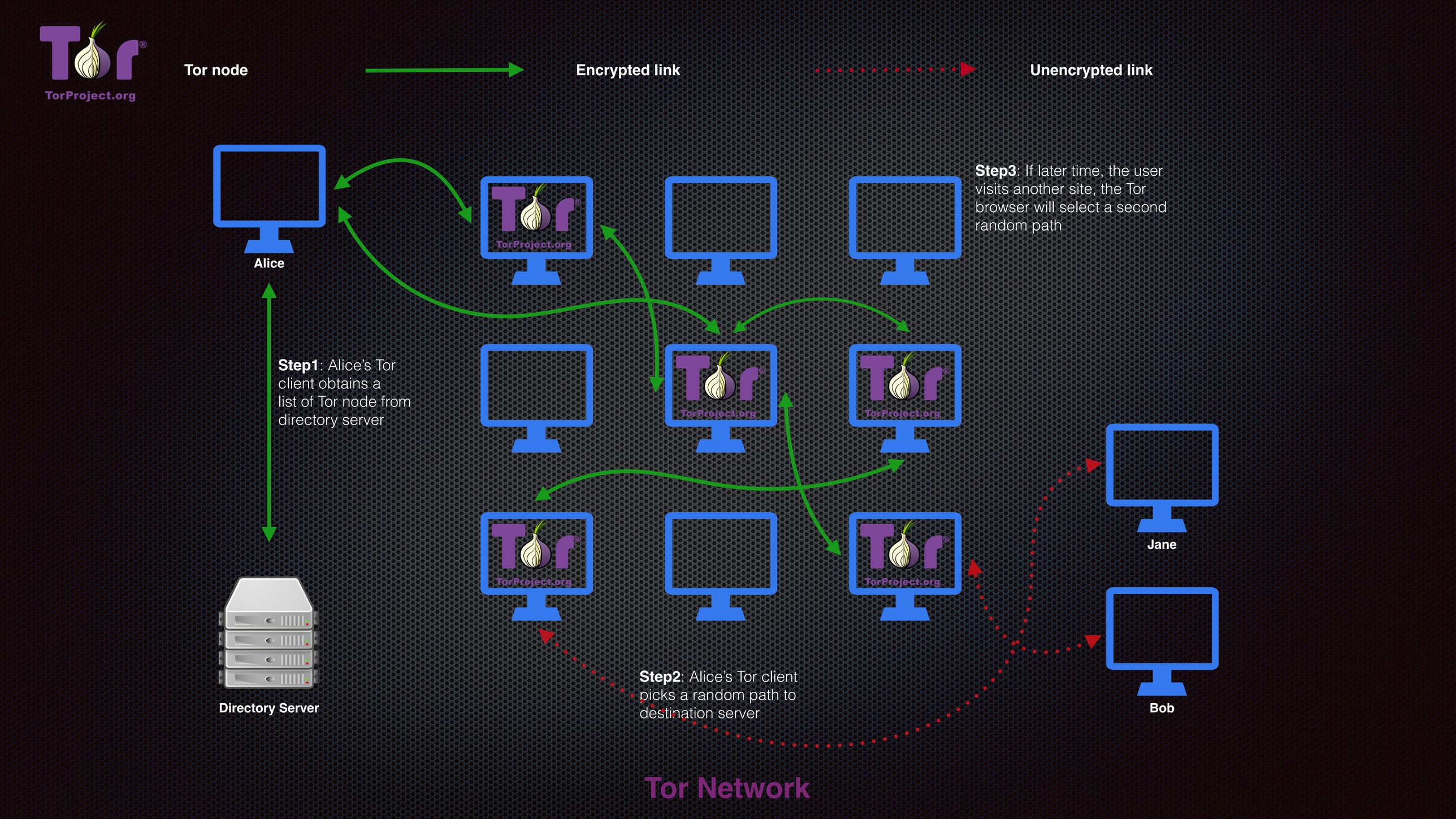
https://metrics.torproject.org/rs.html



Relays in the network that are not listed in the public Tor directory

https://community.torproject.org/relay/types-of-relays/

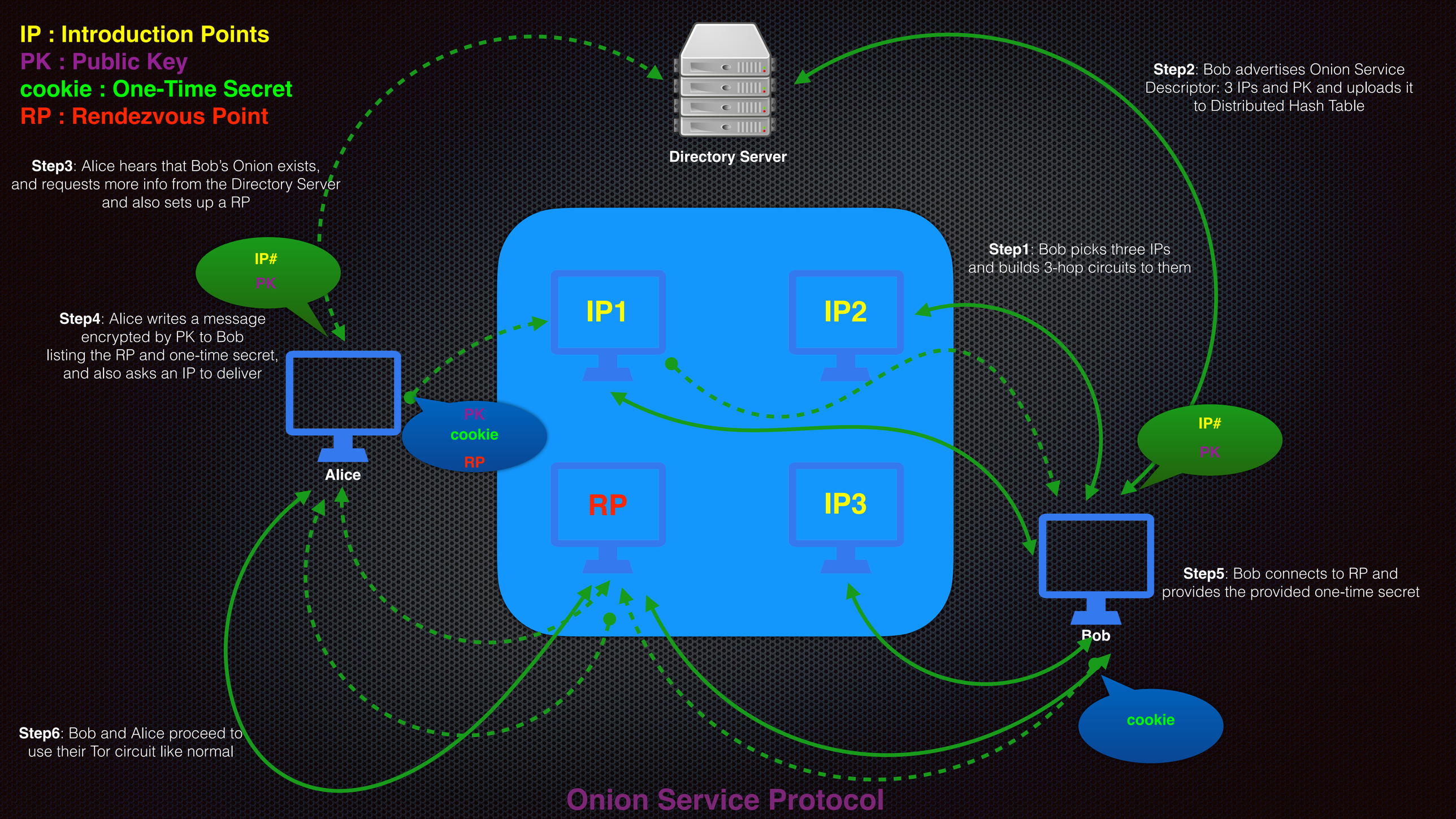
How Tor works


TorProject.org
Tor node
Encrypted link
Unencrypted link
Alice
Step1: Alice's Tor client obtains a list of Tor node from directory server
Step3: If later time, the user visits another site, the Tor browser will select a second random path
Directory Server
Step2: Alice's Tor client picks a random path to destination server
Jane
Bob
Tor Network

Onion Services

- The services are only accessible through the Tor network
- Advantages
  - The service IP and location are hidden
  - All traffic is end-to-end encrypted
  - No need to purchase the domain name
- Disadvantage
  - Slow
  - Blocked in some countries
    - China, Iran

How Onion Services work


IP : Introduction Points
PK : Public Key
cookie : One-Time Secret
RP : Rendezvous Point
Directory Server
Step2: Bob advertises Onion Service Descriptor: 3 IPs and PK and uploads it to Distributed Hash Table
Step3: Alice hears that Bob's Onion exists, and requests more info from the Directory Server and also sets up a RP
Step1: Bob picks three IPs and builds 3-hop circuits to them
IP#
PK
Step4: Alice writes a message encrypted by PK to Bob listing the RP and one-time secret, and also asks an IP to deliver
IP1
IP2
RP
IP3
PK
cookie
RP
Alice
IP#
PK
Bob
Step5: Bob connects to RP and provides the provided one-time secret
cookie
Step6: Bob and Alice proceed to use their Tor circuit like normal
Onion Service Protocol

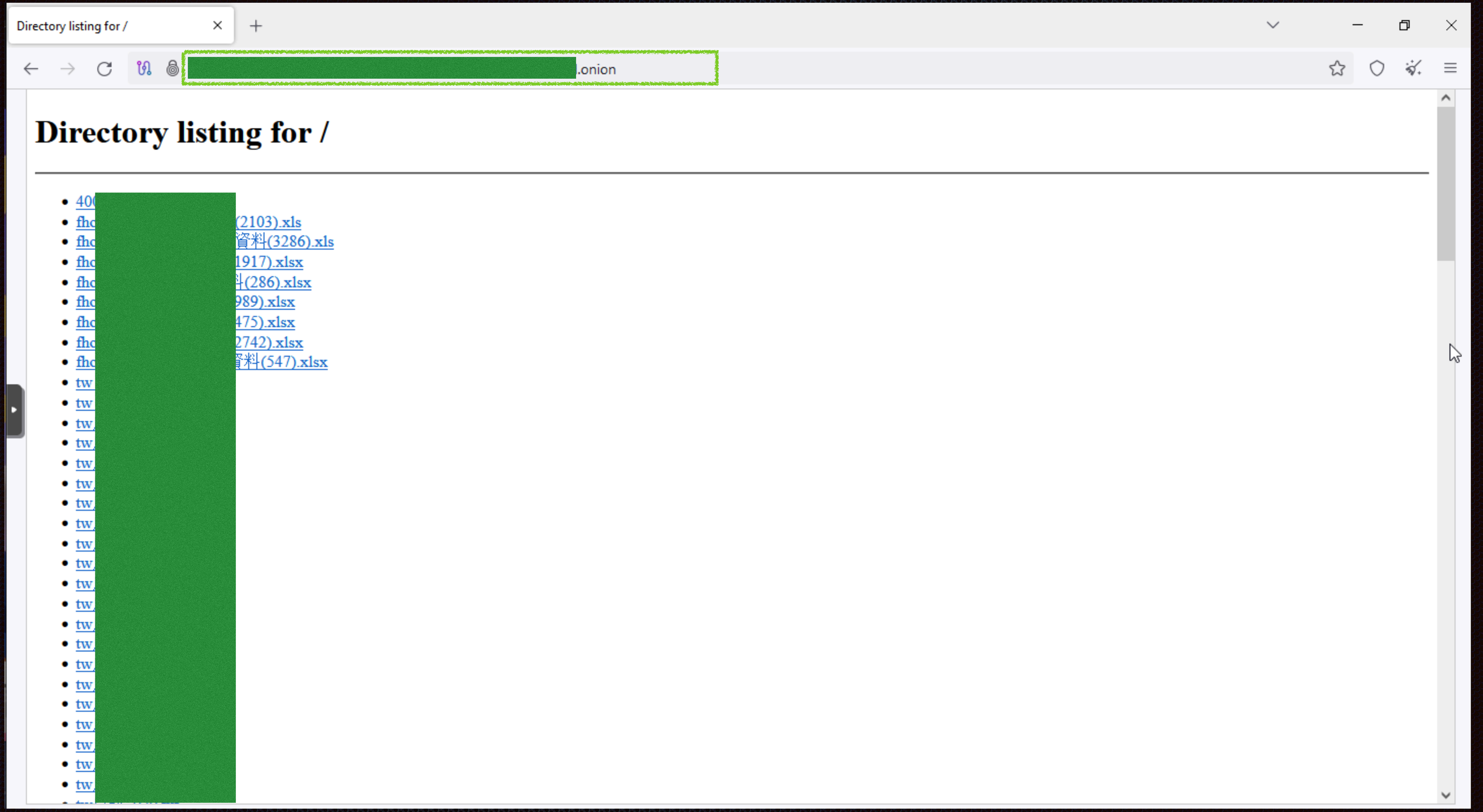
Set Up Your Onion Service

- Set up your regular service
  - Apache or Nginx
- Bind the address to 127.0.0.1 only
- Install Tor
  - https://community.torproject.org/onion-services/setup/install/
- /etc/tor/torrc
  - *HiddenServiceDir /var/lib/tor/YourOnionSrv/*
  - *HiddenServicePort 80 127.0.0.1:80*
- Restart Tor

https://github.com/jieliau/TorSetup

```
jieliau@tempLinux:~/tmp$ python3 -m http.server -b 127.0.0.1 4444
Serving HTTP on 127.0.0.1 port 4444 (http://127.0.0.1:4444/) ...
127.0.0.1 - - [05/May/2024 12:07:06] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [05/May/2024 12:07:09] code 404, message File not found
127.0.0.1 - - [05/May/2024 12:07:09] "GET /favicon.ico HTTP/1.1" 404 -
```

```
jieliau@tempLinux:~/workspaces/TorSetup$ sudo ./torsetup.sh
[sudo] password for jieliau:
Welcome to the Tor Setup.
Hit:1 http://tw.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://tw.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://tw.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 https://download.docker.com/linux/ubuntu jammy InRelease
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 110 kB in 3s (33.8 kB/s)
Reading package lists... Done
Please select which service you want 1) Tor Relay 2) Tor Hidden Service:2
Tor Hidden Service:
Your real service port: 4444
Your hidden service port: 80
Log notice file /var/log/tor/notices.log
Log debug file /var/log/tor/debug.log
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:4444
You onion URL: [redacted].onion
```


Directory listing for /
.onion
Directory listing for /
(2103).xls
資料(3286).xls
1917).xlsx
料(286).xlsx
989).xlsx
475).xlsx
2742).xlsx
資料(547).xlsx

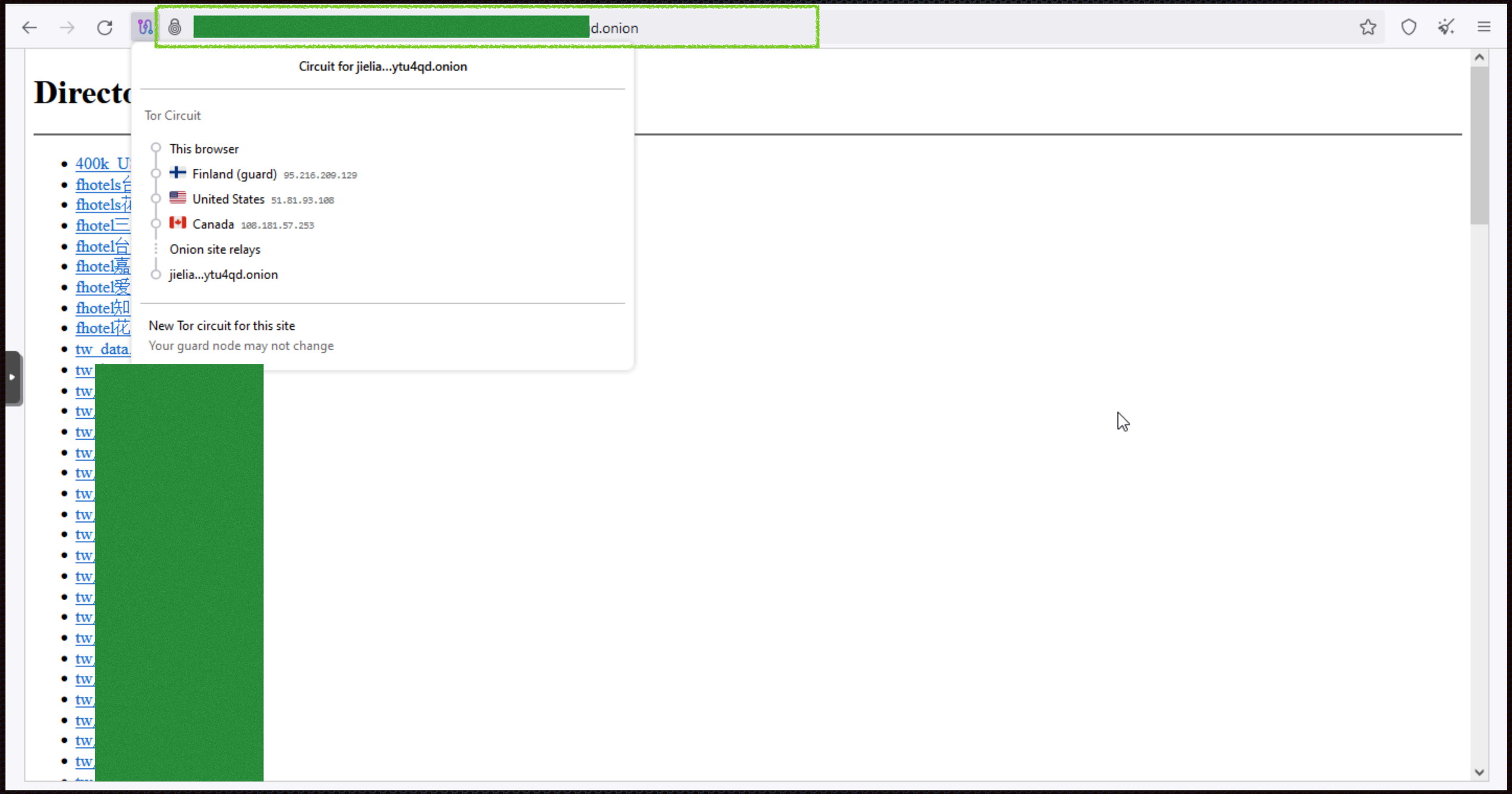
Customise Your onion domain

https://github.com/cathugger/mkp224o

```
jieliau@tempLinux:~/workspaces/mkp224o$ ./mkp224o -d jieliau jieliau
set workdir: jieliau/
sorting filters... done.
filters:
        jieliau
in total, 1 filter
using 4 threads
[redacted].onion
[redacted].onion
```

```
jieliau@tempLinux:~/workspaces/mkp224o$ cd jieliau/
jieliau@tempLinux:~/workspaces/mkp224o/jieliau$ ls
[redacted]
jieliau@tempLinux:~/workspaces/mkp224o/jieliau$ cd [redacted]
jieliau@tempLinux:~/workspaces/mkp224o/jieliau[redacted]
hostname  hs_ed25519_public_key  hs_ed25519_secret_key
jieliau@tempLinux:~/workspaces/mkp224o/jieliau/[redacted]onion$ sudo cp * /var/lib/tor/hidden_service/
```

```
root@tempLinux:/var/lib/tor/hidden_service# pwd
/var/lib/tor/hidden_service
root@tempLinux:/var/lib/tor/hidden_service# ls -l
total 20
drwx--S--- 2 debian-tor debian-tor 4096 五    5 12:05 authorized_clients
drwxr-sr-x 2 debian-tor debian-tor 4096 五    5 15:31 hdsrv_bkp
-rw-r--r-- 1 debian-tor debian-tor   63 五    5 15:32 hostname
-rw-r--r-- 1 debian-tor debian-tor   64 五    5 15:32 hs_ed25519_public_key
-rw------- 1 debian-tor debian-tor   96 五    5 15:32 hs_ed25519_secret_key
root@tempLinux:/var/lib/tor/hidden_service# cat hostname
[redacted].onion
root@tempLinux:/var/lib/tor/hidden_service#
```


[redacted]d.onion
Circuit for jielia...ytu4qd.onion
Tor Circuit
This browser
Finland (guard) 95.216.209.129
United States 51.81.93.108
Canada 108.181.57.253
Onion site relays
jielia...ytu4qd.onion
New Tor circuit for this site
Your guard node may not change
Directo
400k_U
fhotels台
fhotels花
fhotel三
fhotel台
fhotel嘉
fhotel爱
fhotel知
fhotel花
tw_data
[redacted]

OSINT

- x.com
  - (url:onion) “ransomware”
  - ransomware AND (url:onion -filter:retweets)
  - (hxxp:// OR http://) [.] AND url:onion
  - target OR dump OR combo OR password OR leak OR breach OR databreach OR credential OR steal AND (url:onion)
- Google Dorks
  - Intext:.onion site:reddit.com
- Reddit
  - r/TOR
  - r/onions
- Shodan
  - ssl:”.onion”
  - “.onion”
  - “facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion”

Home
Explore
Notifications
Messages
Lists
Bookmarks
Communities
Premium
Profile
More
Post

Jie Liau
@0xJieLiau

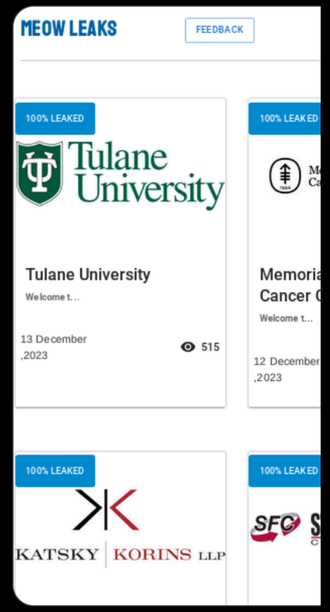
OR databreach OR credential OR steal AND (url:onion)

Top Latest Pe

RAKESH KRISHNAN @RakeshKri
#MeowRansomware announced 1
#dataleaks on surface & dark web

meowleak./co
...lr2g4ltxsh3rbbx7kfrp4l55u4i7xy
...32glgkp2ejeqlnx5ynnxvbebgnle

#ransomware #malware #cybera
#darkweb #deepweb #meow #da



1

Багровый Гройпер @InchP965
Wednesday meme **dump**, enjoy.

...ecudq444woadhzr2plxlaayexnh

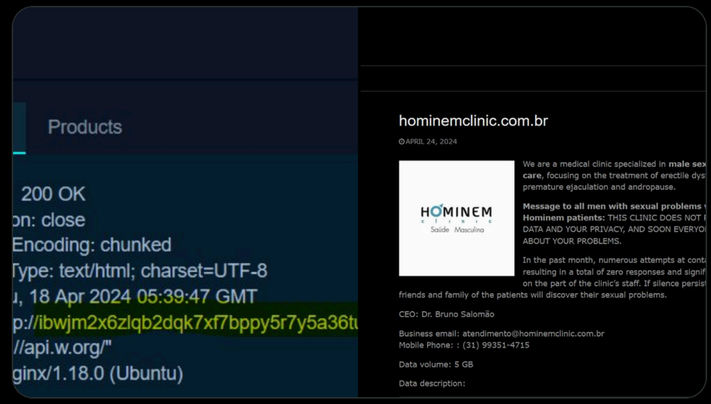
Trending in Taiwan

ransomware AND (url:onion -filter:retweets)

Top Latest People Media Lists

...r7y5a36tuci4bx4fgqmmihp7he7flyd.onion
IP:94.156.79.124
nginx/1.18.0 (Ubuntu)

Main Domain of #Qiulong: ...qnon54gjns5nmag3hmqv6fcwamtkmad.onio...
Show more



4 8 38 5.7K

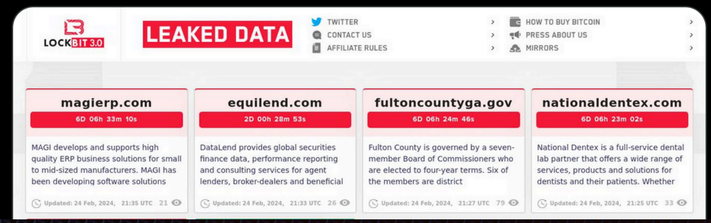
RAKESH KRISHNAN @RakeshKrish12 · Feb 25
#LockBit is back online as LockbitSupp using decentralised infrastructure!

Listed 5 new Victims!

Claimed to have exploited PHP Vuln CVE-2023-3824 by FBI. Patched

...2vieqbujxw7rd6ofzdtapjb4rrawqad.onion

...mltipntwlkmidcll2qirbu7ykg46eyd.onion
...
Show more



Search filters

People
From anyone
People you follow

Location
Anywhere
Near you

Advanced search

Trends for you

Trending in Taiwan
#AI美女
12.9K posts

Trending in Taiwan
#UnknownTheSeries
2,153 posts

Celebrities · Trending
Anne Hathaway
26.4K posts

Trending in Taiwan
Most Handsome Man Alive
30.9K posts

Trending in Taiwan
Germany
121K posts

Trending in Taiwan
TSMC

Messages

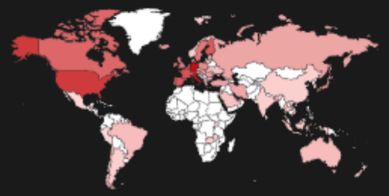
Shodan Your Real IP

SHODAN | Explore | Downloads | Pricing | .onion

TOTAL RESULTS

3,817

TOP COUNTRIES



Germany	971
Italy	783
United States	388
France	231
Netherlands	204

More...

TOP PORTS

443	2,891
8443	499
80	296
8080	13
25	8

More...

TOP ORGANIZATIONS

Hetzner Online GmbH	489
Aruba S.p.A. - Cloud Services IT3	167
DigitalOcean, LLC	138

View Report | Download Results | Historical Trend | Browse Images | View on Map

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]

Riseup Networks

United States, Seattle

hljs

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
share.riseup.net

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 04 May 2024 07:41:32 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1452
Connection: keep-alive
Accept-Ranges: bytes
Last-Modified: Wed, 11 Mar 2020 20:37:14 GMT
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src ...
```

301 Moved Permanently

[redacted]

Sweden, Stockholm

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
mullvad.net

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Sat, 04 May 2024 07:37:37 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://mullvad.net/
Strict-Transport-Security: max-age=15768000; includeSubDomains
Onion-Location: http://o54hon2e2vj6c7m3aqqu6uye...
```

GlobaLeaks

[redacted]

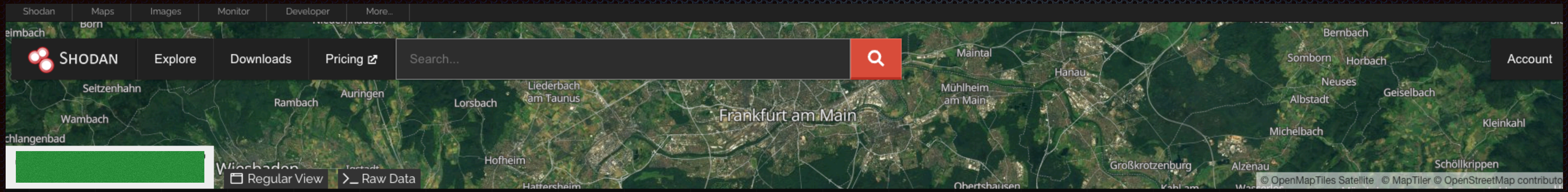
cloud | self-signed

SSL Certificate

Issued By:
|- Common Name:
127.0.0.1

Issued To:
|- Common Name:

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: GlobaLeaks
Date: Sat, 04 May 2024 07:35:09 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Onion-Location: http://74ol7msveocytfheettmcataiud3gerrhavivivifrig4vodk42qx5qd.onion/
Content-Security-Policy: base-uri ...
```



// TAGS: cloud

// LAST SEEN: 2024-05-04

General Information

Hostnames	[redacted]
Domains	AMAZONAWS.COM, HOSSEIN.BLOG
Cloud Provider	Amazon
Cloud Region	eu-central-1
Cloud Service	EC2
Country	Germany
City	Frankfurt am Main
Organization	A100 ROW GmbH
ISP	Amazon.com, Inc.
ASN	AS16509

Open Ports

nginx 1.24.0

```
HTTP/1.1 200 OK
Server: nginx/1.24.0
Date: Sun, 28 Apr 2024 01:52:49 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
vary: Accept-Encoding
vary: Accept, Accept-Language, Cookie
x-frame-options: DENY
x-content-type-options: nosniff
x-xss-protection: 0
referrer-policy: same-origin
[redacted]
x-cached: MISS
onion-location: http://[redacted]xqd.onion/
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=SOS3AojKJDJbvG0Z%2BcCIjRf9FSdeudVSJLOxYNy2mpIfoPumE4%2FHnY8XN5XdfEiIjFcQJNRWHYgH7vRYOlSxgwVRiX51XqHe1IXj0R%2BgoXZax1RTT5hi2FBYmFfVXMIF6OWu"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
CF-RAY: 87b36a42786e9183-FRA
alt-svc: h3=":443"; ma=86400
```

Not Secure

Search

Explore

Posts Hashtags News

kolektiva.social is part of the decentralized social network powered by Mastodon.

Kolektiva is an anti-c
that offers federated
collectives and indiv
the social movemen

ADMINISTERED BY:

admin
@admin

mastodon

Explore

These are posts from across the social web that are gaining traction today.

Explore - kolektiva.social

Search

Explore

Posts Hashtags News

kolektiva.social is part of the decentralized social network powered by Mastodon.

These are posts from across the social web that are gaining traction today.
Newer posts with more boosts and favorites are ranked higher.

Kolektiva is an anti-colonial anarchist collective that offers federated social media to anarchist collectives and individuals in the fediverse. For the social movements and liberation!

ADMINISTERED BY:

admin
@admin

SERVER STATS:

3.9K
active users

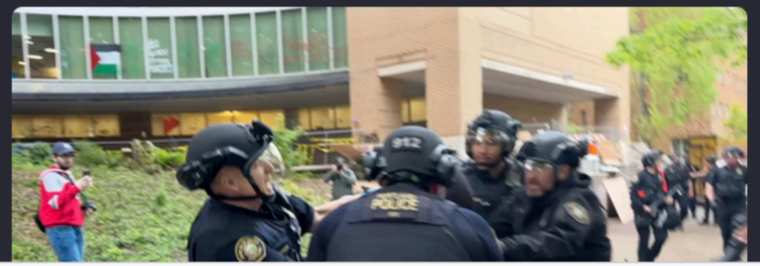
Learn more

kolektiva.social: About · Profiles directory · Privacy policy

Mastodon: About · Get the app · Keyboard shortcuts · View source code · v4.2.8

Alissa Azar
@alissaazar
18h

Here's the last video I took as they arrested me. It hasn't been edited, but it is clipped/shortened because some of the folks don't want their violent arrest footage online. As you can see I was just filming, and what's not really shown here is that I was surrounded by other press and photographers. He told me to leave yet arrested me immediately. Other cop also kept telling me to "stop" and not resist even though I wasn't doing anything and my hands were already in cuffs as he was saying that.
During this wave of arrests 8 of us were grabbed. Many while trying to get out of the area but they just grabbed whoever they could. My arrest is pretty tame but everyone else that I saw was pretty brutal with so many cops on one person.



mastodon

Explore

Login to follow profiles or hashtags, favorite, share and reply to posts. You can also interact from your account on a different server.

Create account

Login

https://github.com/jieliau/TorSetup/blob/master/shodanOnion.py

Analyse Onion Site

- Set up Tor Proxy
  - /etc/tor/torrc
    - *SocksPort 0.0.0.0:9050*
    - *SocksPolicy accept 192.168.0.0/16*
    - *SocksPolicy reject **
- *torify(torsocks)* or *proxychain*

zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

create account log in

main page | discussion | view source | history

The Hidden Wiki

navigation

- Main page
- Recent changes
- Random page
- Rules of the site

search

Search The Hidden Wiki

Go Search

tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Main Page

Welcome to The Hidden Wiki! Our official Hidden Wiki url in 2024 is:
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
Add it to bookmarks and spread it!!!!!!

The Official Hidden Wiki 2024 contest is ON!!

Now You can earn FREE MONEY with the Hidden Wiki!

Click HERE to learn how!

Contents [hide]

Editor's picks

Pick a random page from the article index and replace one of these slots with it:

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.
4. In Praise Of Hawala - Anonymous informal value transfer system.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer

Volunteer

Here are the six different things that you can help us out with:

1. Plunder other hidden service lists for links and place them here!
2. File the SnapBBSIndex links wherever they go
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum.
5. Perform Dead Services Duties
6. Remove CP shitness.

Introduction Points

- Ahmia.fi - Clearnet search engine for Tor Hidden Services.
- DuckDuckGo - A Hidden Service that searches the clearnet

```
┌──(jieliau㉿kali)-[~/workspace/CVE-2024-3400]
└─$ torsocks -a 192.168.0.4 -p 9050 dirb http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/

-----------------

DIRB v2.22
By The Dark Raver

-----------------

START_TIME: Sun May  5 15:11:48 2024
URL_BASE: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/ ----
1714893228 ERROR torsocks[3393166]: Connection timed out (in socks5_recv_connect_reply() at socks5.c:547)
+ http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/html/
+ http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/index.html (CODE:200|SIZE:0)
+ http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/index.php (CODE:200|SIZE:374)
+ http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/robots.txt (CODE:200|SIZE:0)
==> DIRECTORY: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wa/
==> DIRECTC
```

```
┌──(jieliau㉿kali)-[~]
└─$ torsocks -a 192.168.0.4 -p 9050 nikto -host http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          127.42.42.0
+ Target Hostname:    zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
+ Target Port:        80
+ Start Time:         2024-05-05 16:20:56 (GMT8)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.php, /index.html
+ Uncommon header 'x-request-id' found, with contents: 0a959312dcea9e673bd1e1c2
+ 7790 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-05-05 21:15:15 (GMT8) (17659 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Monitor Your Data on DarkWeb


WHAT ARE YOU DOING ON THE DARK WEB??
I FORGOT MY PASSWORD, SO I'M LOOKING IT UP.
Bathstein/MORGAN 2021
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

AIL Framework

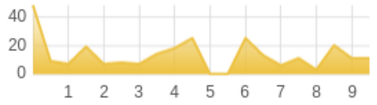
The framework for Analysis of Information Leaks

To analyse potential information leaks from unstructured data sources including DarkWeb

https://github.com/ail-project/ail-framework

Toggle Sidebar

Total pastes since 10 min



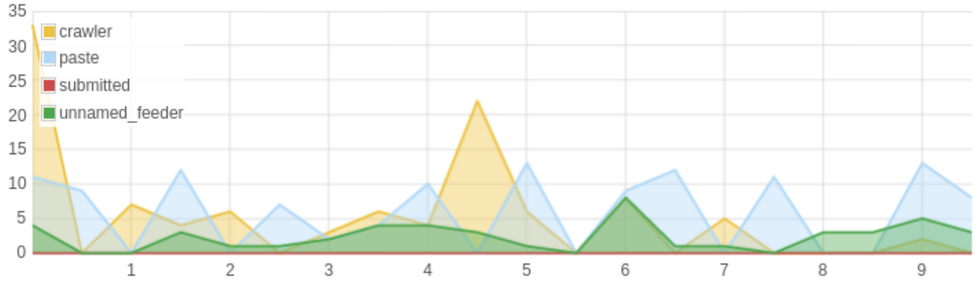
Display queues

Idling queues
Working queues
Stuck queues

Queue Name.PID	Amount
ApiKey.1495283	0
Categ.1495199	0
Crawler.1495254	0
Credential.1495292	1
CreditCards.1495299	5
Cryptocurrencies.1495305	0
CveModule.1495311	0
D4Client.1495152	0
Decoder.1495318	0
DomClassifier.1495540	44283812
Duplicates.1495340	0
FeederModuleImporter.1495147	0
Global.1495179	0
Hosts.1495533	0
IPAddress.1495384	198611
Iban.1495362	0
Indexer.1495220	0
Keys.1495406	0
Languages.1495427	0
LibInjection.1495608	23
MISP_Thehive_Auto_Push.1495666	0
Mail.1495450	0
Mixer.1495172	0

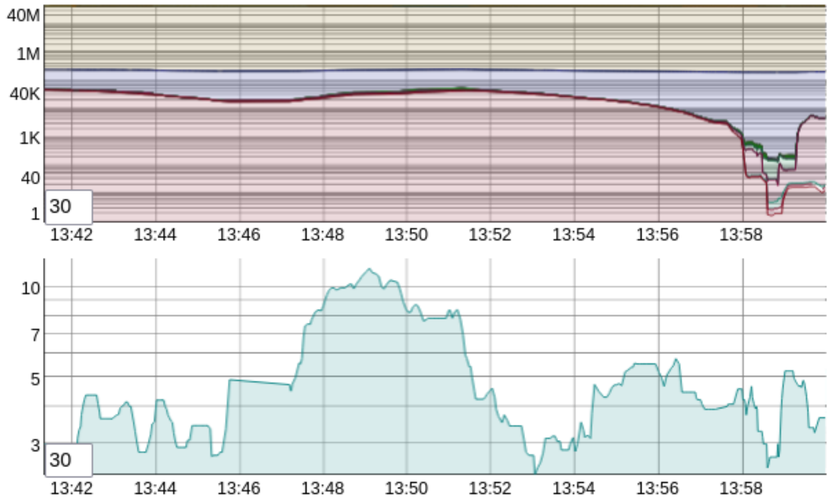
Feeder(s) Monitor:

Processed items



Filtered duplicates

Queues Monitor

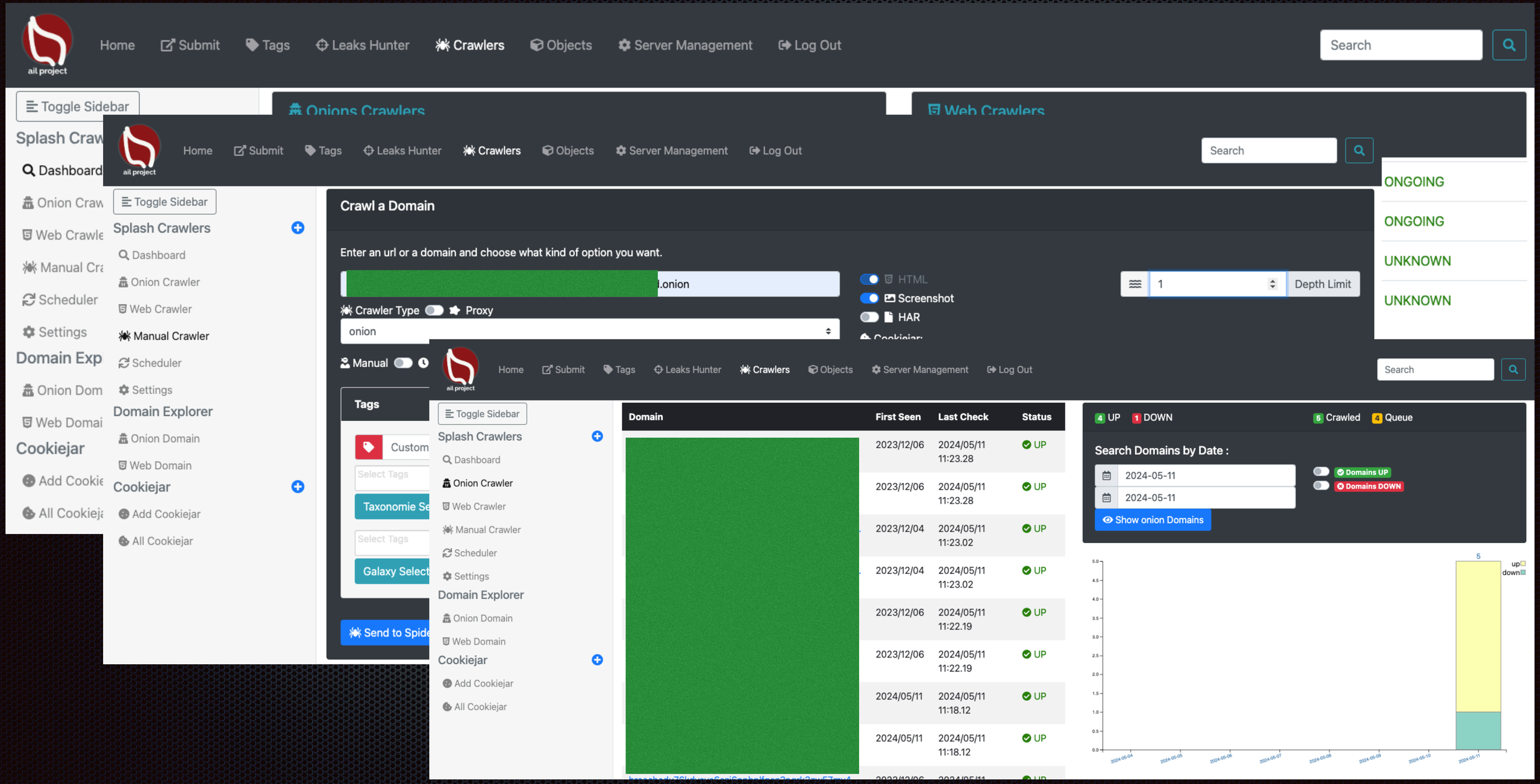


Logs

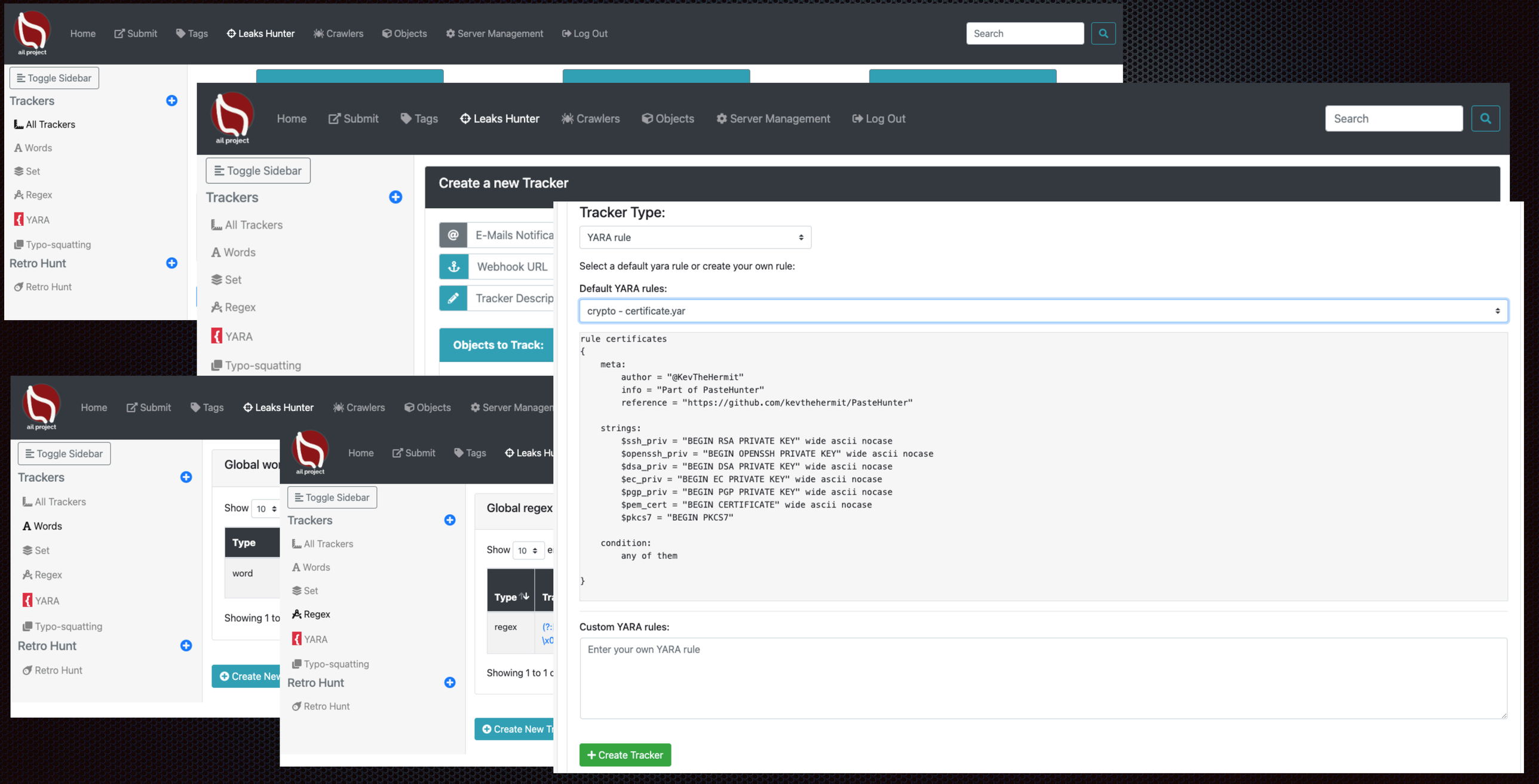
15 INFO WARNING CRITICAL

Time	Channel	Level	Script Name	Source	Date	Paste name	Message	Actions
08:42:42	Script	WARNING	CreditCard	archive/pastebin.com_pro	20230531	KWnBqXh9.gz	Checked 1 valid number(s)	
08:45:47	Script	WARNING	Credential	crawled	20230531	7kd5gvuzuu44obhhghomhr4sisjfbrpw5bkcofjqknmxx6sfcw3rerid.onionc5fd0810-6791-4198-a3e8-55865a32aa87	Checked 9 credentials found. Related websites: http://onionmail.info/directory.html	
09:21:02	Script	WARNING	Mails	crawled	20230531	sou4vla4k5peskbl3dlzhh3e6ve5eu3m3hhsmiidqevlsd6lqo3qq2ad.onion76075609-d359-4d75-8147-2ec46f763752	Checked 20 e-mail(s)	
09:30:36	Script	WARNING	Mails	archive/pastebin.com_pro	20230531	qKLtd3As.gz	Checked 24 e-mail(s)	
09:36:56	Script	WARNING	Iban	archive/pastebin.com_pro	20230531	JfTMNpmR.gz	Checked found 1 IBAN	
09:40:18	Script	WARNING	CreditCard	archive/gist.github.com	20230531	Anjum48_38cddcf1082295935c0d2d63daac69c3.gz	Checked 1 valid number(s)	
09:55:03	Script	WARNING	CreditCard	archive/pastebin.com_pro	20230531	wR6vVzzS.gz	Checked 4 valid number(s)	

Crawlers


ail project
Home
Submit
Tags
Leaks Hunter
Crawlers
Objects
Server Management
Log Out
Search
Toggle Sidebar
Splash Crawlers
Dashboard
Onion Crawler
Web Crawler
Manual Crawler
Scheduler
Settings
Domain Explorer
Onion Domain
Web Domain
Cookiejar
Add Cookiejar
All Cookiejar
Onions Crawlers
Web Crawlers
Crawl a Domain
Enter an url or a domain and choose what kind of option you want.
.onion
Crawler Type
Proxy
onion
HTML
Screenshot
HAR
1
Depth Limit
Manual
Tags
Custom
Select Tags
Taxonomie Se
Galaxy Select
Send to Spide
ONGOING
ONGOING
UNKNOWN
UNKNOWN
Domain
First Seen
Last Check
Status
2023/12/06
2024/05/11 11:23.28
UP
2023/12/04
2024/05/11 11:23.02
2024/05/11
2024/05/11 11:18.12
4 UP
1 DOWN
5 Crawled
4 Queue
Search Domains by Date :
2024-05-11
Domains UP
Domains DOWN
Show onion Domains
up
down

Leaks Hunter



Your Own DarkWeb monitor

requests-tor Python module

```
jieliau@tempLinux:~$ python3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from requests_tor import RequestsTor
>>> rt = RequestsTor(tor_ports=(9050,))
>>> url = 'http://                                                    .onion'
>>> res = rt.get(url)
>>> res.status_code
200
>>> res.text
'<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">\n<html>\n<head>\n<meta http-equiv
```

https://pypi.org/project/requests-tor/

Tor Sites

breache[redacted]onion/Announcement-Database-Index

Databases | Upgrades | Search | Hidden Service | Escrow | + Extras

BreachForums > Leaks > Forum Announcement

Mark all as read | Today's posts

Forum Announcement: Database Index

[Admin] Hollow

Administrator

ADMINISTRATOR

S

Posts:	65
Threads:	3
Joined:	Jun 2023

01-08-2023, 12:14 PM

This thread will index all the datasets we have marked as "Official" meaning they are verified by an admin and kept online 24/7/365 via our CDN.
Please note there are hundreds more unofficial datasets in the Databases subforum.
This list is not only limited to database breaches, you will find some combolists here too.

Join our Telegram for notifications when a new breach is added into our official library - **https://t.me/breachforums_cdn**.

Lifetime Access

Sorting options:

- Record Count: [**HIGHER-LOWER**] [**LOWER-HIGHER**]
- Date Added: [**NEWER-OLDER**] [**OLDER-NEWER**]
- Breach Date: [**NEWER-OLDER**] [**OLDER-NEWER**]
- Title: [**A-Z**] [**Z-A**]

Click here to learn how to get credits.
Click here to view some basic rules.

We have a total of 15,638,174,793 Records from the following 975 Datasets, free for download once you unlock them.
[014,936,670] | 2015 - *(000webhost.com)* 000webhost Database ➡ Download Here!
[007,476,940] | 2021 - *(datpiff.com)* DatPiff Database ➡ Download Here!
[007,633,234] | 2018 - *(blankmediagames.com)* BlankMediaGames Database ➡ Download Here!
[015,003,961] | 2021 - *(epik.com)* Epik Database ➡ Download Here!

dread[redacted].onion

dread

frontpage all dread

Login or Register

1 How do I create an account on jabber.calyxinstitute.org if I don't have a desktop, laptop, or a computer of any chance and I only have a phone for ins

by /u/Steal_Shifter • 9 hours ago in /d/DarkNetMarkets

1 comments

1 looking for "hackers , blackhats , cyber security " communities

by /u/hyechjo789 • 10 hours ago in /d/hacking

1 comments

1 Oneplus FRP Bypass?

by /u/PublicBug1738 • 10 hours ago in /d/hacking

3 comments

1 i need my gf's following list on instagram but she wont let me see

by /u/yorboi • 10 hours ago in /d/hacking

14 comments

2 LocalMonero closing, what now?

by /u/RaccoonBandit • 12 hours ago in /d/OpSec

17 comments

1 Quenstion about efficient Monero Purchase methods for Bank Accounts and PayPal Access

by /u/kenzodeep87 • 12 hours ago in /d/OpSec

1 comments

2 I think the FBI is on dread

by /u/riseabove444 • 14 hours ago in /d/OpSec

Suggestions

/d/Dread
355,367 subscribers

/d/DarkNetMarkets
110,339 subscribers

/d/HarmReduction
4,768 subscribers

/d/DarknetMarketsNoobs
49,370 subscribers

/d/hacking
49,373 subscribers

/d/OpSec
57,757 subscribers

/d/Monero
39,518 subscribers

/d/Recon
10,755 subscribers

/d/EnergyControl

tor66 [redacted] iid.onion

TOR66

Random Onions Fresh Onions

Search and Find .onion websites ...

Search what you mind... Search

Fresh Onions | TOP# Onions

Promoted sites

ransomw[redacted].onion

120%

Ransomware Group Sites

If you want to buy me a coffee for my work, donations are warm welcome to one of those addresses:
DOGE: DBPbrvFShnykgBa8svQ91F9Vgs1zhhgmB1
LTC: LXMDziBcT474Mava74r9BvkTyoXcaUk6MD
BTC/BCH: 1FyCD8kp9ekiTTgdyhFtZRgzR1QCHV4i84
XMR: 48FgeW4fUpyjPDGxJdHaA441F5c9szYtLSVWbNv8T3ZXe9ZN3iLUSSdASof2vDQqdbgRYom9aMeQMWPQkr3SPZUJE2uM8fc

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open | DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open | Open
Medusa	v3	Open

Ransomware Group Sites | LockBit BLOG | dark.fail: Which Tor sites are onl

lockbit[redacted]on/page3.php

SEIZED LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency | FBI | EUROPOL

Press Releases

PUBLISHED

Updated: 02 May, 2024, 13:37 BST 2465

Who is LockbitSupp?

PUBLISHED

Updated: 02 May, 2024, 13:37 BST 3060

But there's more...

PUBLISHED

Updated: 02 May, 2024, 13:37 BST 2330

What have we learnt?

PUBLISHED

Some facts and figures from the backend!

NCA National Crime Agency | LOCKBIT 3.0

Updated: 02 May, 2024, 13:37 BST 2083

More LB hackers exposed

PUBLISHED

After compromising Lockbit's platform, Law Enforcement will be coordinating activity to deal with Lockbit's affiliates.

Updated: 02 May, 2024, 13:37 BST 2126

What have we been doing?

PUBLISHED

Supporting victims worldwide!

Updated: 02 May, 2024, 13:37 BST 1736

Preventing and protecting

PUBLISHED

National Cyber Security Centre
a part of GCHQ

Updated: 02 May, 2024, 13:37 BST 1525

Report Cyber Attacks!

PUBLISHED

Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement.

Updated: 02 May, 2024, 13:37 BST 1502

Close

1D 19H 3M 39S


IT'S SIMPLE
I hope you enjoy it
YOU TURN YOUR LIGHTS OFF