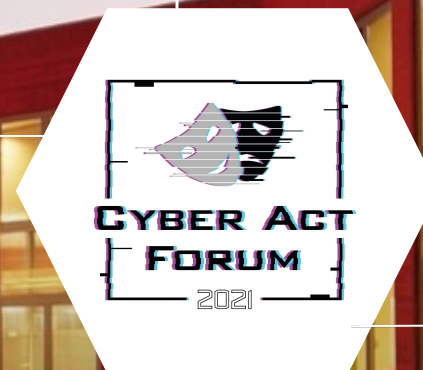




# ILLUMINIAMO IL DARK WEB

## Massimo Giaimo

# Dark what?

## Surface Web

Indexed content (50 billion pages).

Can be found with traditional search engines  
and accessed with traditional browsers

## Deep Web

Unindexed content (96-99% entire internet).

Cannot be found with traditional search engines.

## Dark Web

Intentionally hidden content.

Can be accessed with special software.

1-4% of the entire internet

## Networks

friend-to-friend, Tor, Freenet,

I2P, Riffle, Netsukuku

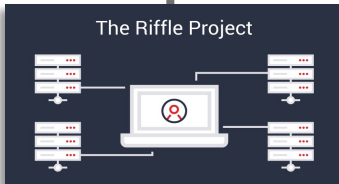
- <https://www.csoononline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html>
- <https://siteefy.com/how-many-websites-are-there/>
- <http://netsukuku.freaknet.org/>

# How to start?



<https://www.torproject.org/download/>

<https://geti2p.net/it/>



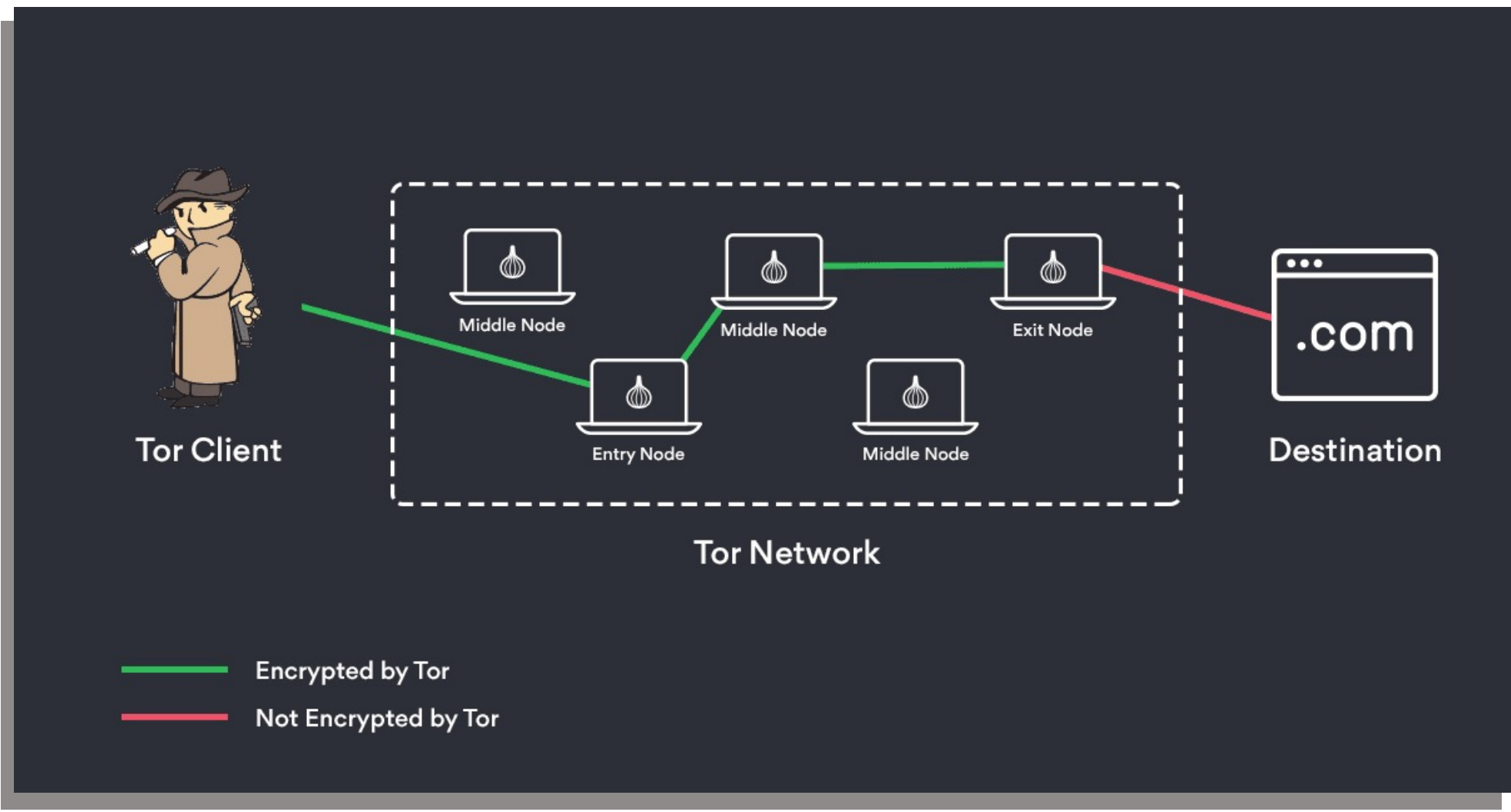
<https://github.com/kwonalbert/<riffle>  
<https://people.csail.mit.edu/devadas/pubs/riffle.pdf>

<https://freenetproject.org/pages/download.html>



#WEINNOVATE

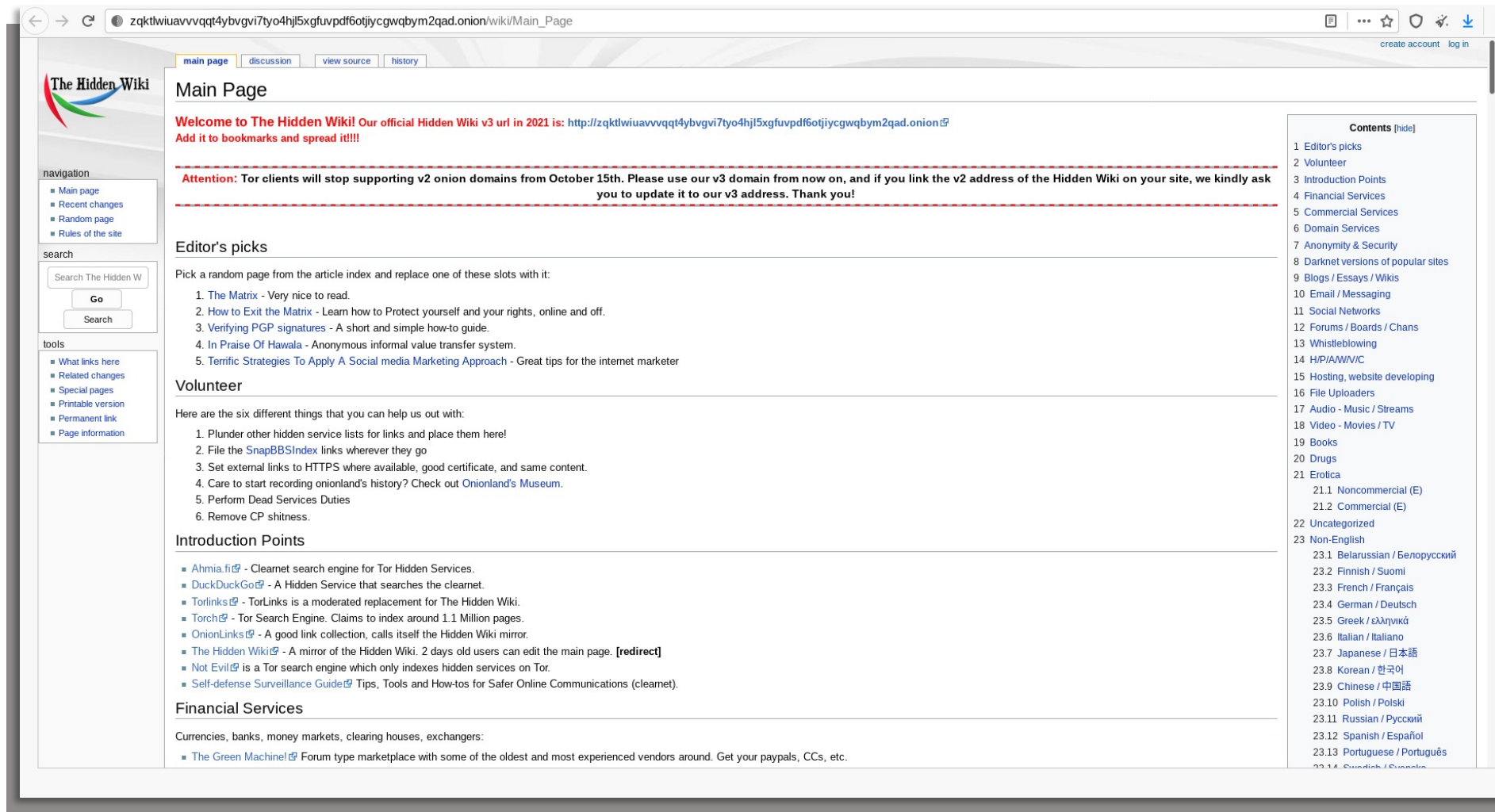
# How to TOR network work



#WEINNOVATE

Image from: <https://ourcodeworld.com/articles/read/953/how-to-route-all-the-machine-traffic-through-tor-in-kali-linux>

# Look for sources – hidden services directories



The screenshot shows the main page of The Hidden Wiki, a directory of hidden services. The page is viewed in a web browser with the URL `zqktlwuavvvqqt4ybvvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbybm2qad.onion/wiki/Main_Page`. The page layout includes a sidebar with navigation links (Main page, Recent changes, Random page, Rules of the site), a search box, and a tools section. The main content area is titled "Main Page" and contains a welcome message, a warning about v2 onion domains, and sections for "Editor's picks", "Volunteer", "Introduction Points", and "Financial Services". The "Introduction Points" section lists various search engines and mirrors. The "Financial Services" section mentions currencies, banks, and a marketplace.

**Main Page**

Welcome to The Hidden Wiki! Our official Hidden Wiki v3 url in 2021 is: <http://zqktlwuavvvqqt4ybvvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbybm2qad.onion>  
Add it to bookmarks and spread it!!!!

**Attention:** Tor clients will stop supporting v2 onion domains from October 15th. Please use our v3 domain from now on, and if you link the v2 address of the Hidden Wiki on your site, we kindly ask you to update it to our v3 address. Thank you!

**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](#) - Clearmet search engine for Tor Hidden Services.
- [DuckDuckGo](#) - A Hidden Service that searches the clearnet.
- [Torlinks](#) - TorLinks is a moderated replacement for The Hidden Wiki.
- [Torch](#) - Tor Search Engine. Claims to index around 1.1 Million pages.
- [OnionLinks](#) - A good link collection, calls itself the Hidden Wiki mirror.
- [The Hidden Wiki](#) - A mirror of the Hidden Wiki. 2 days old users can edit the main page. [\[redirect\]](#)
- [Not Evil](#) is a Tor search engine which only indexes hidden services on Tor.
- [Self-defense Surveillance Guide](#) Tips, Tools and How-tos for Safer Online Communications (clearnet).

**Financial Services**

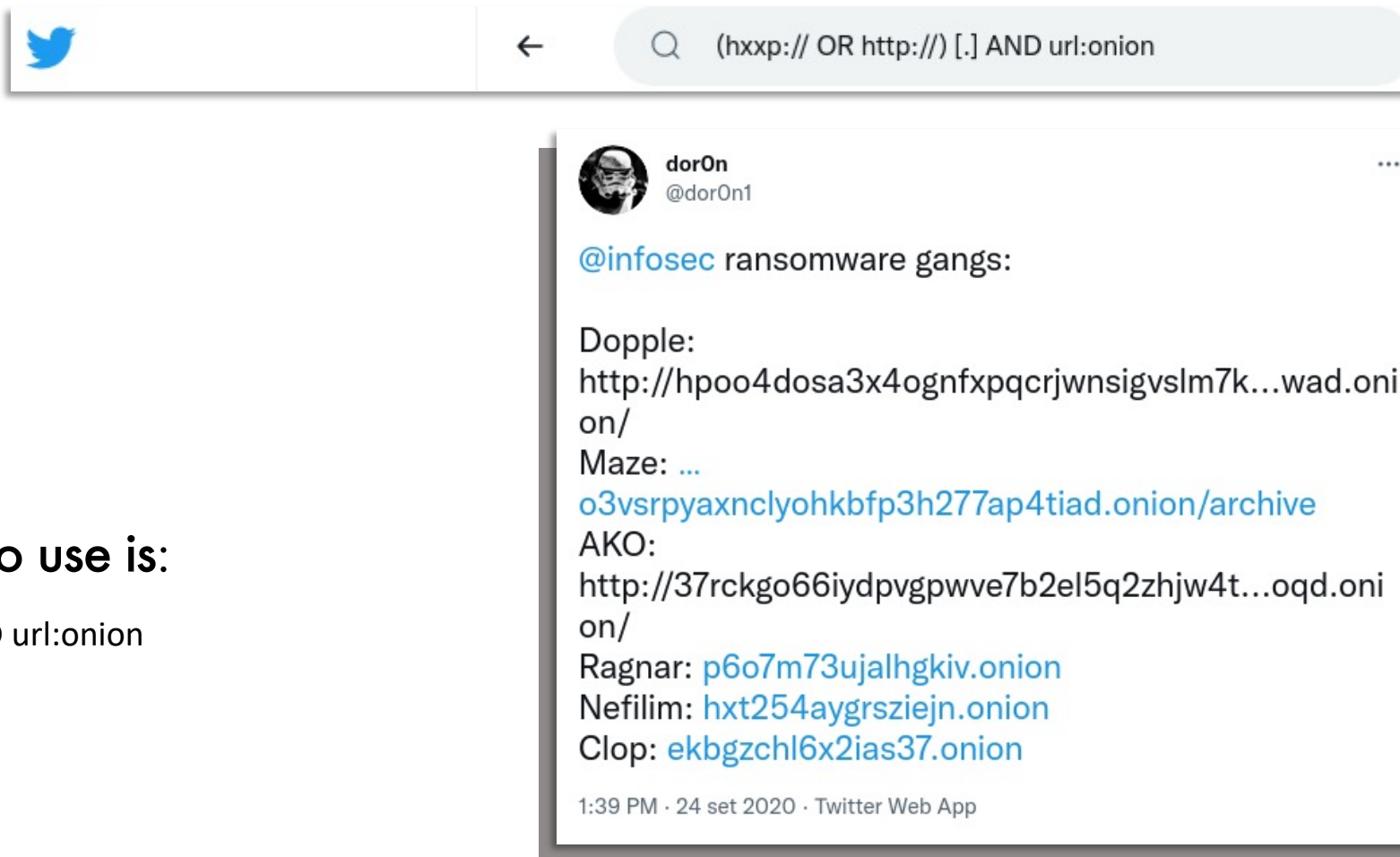
Currencies, banks, money markets, clearing houses, exchangers:

- [The Green Machine!](#) Forum type marketplace with some of the oldest and most experienced vendors around. Get your paypals, CCs, etc.

**Contents [hide]**

- 1 Editor's picks
- 2 Volunteer
- 3 Introduction Points
- 4 Financial Services
- 5 Commercial Services
- 6 Domain Services
- 7 Anonymity & Security
- 8 Darknet versions of popular sites
- 9 Blogs / Essays / Wikis
- 10 Email / Messaging
- 11 Social Networks
- 12 Forums / Boards / Chans
- 13 Whistleblowing
- 14 H/P/A/W/V/C
- 15 Hosting, website developing
- 16 File Uploaders
- 17 Audio - Music / Streams
- 18 Video - Movies / TV
- 19 Books
- 20 Drugs
- 21 Erotica
  - 21.1 Noncommercial (E)
  - 21.2 Commercial (E)
- 22 Uncategorized
- 23 Non-English
  - 23.1 Belarussian / Беларусский
  - 23.2 Finnish / Suomi
  - 23.3 French / Français
  - 23.4 German / Deutsch
  - 23.5 Greek / ελληνικά
  - 23.6 Italian / Italiano
  - 23.7 Japanese / 日本語
  - 23.8 Korean / 한국어
  - 23.9 Chinese / 中国語
  - 23.10 Polish / Polski
  - 23.11 Russian / Русский
  - 23.12 Spanish / Español
  - 23.13 Portuguese / Português
  - 23.14 Swedish / Svenska

# Look for sources - Twitter



- The Twitter Dork to use is:

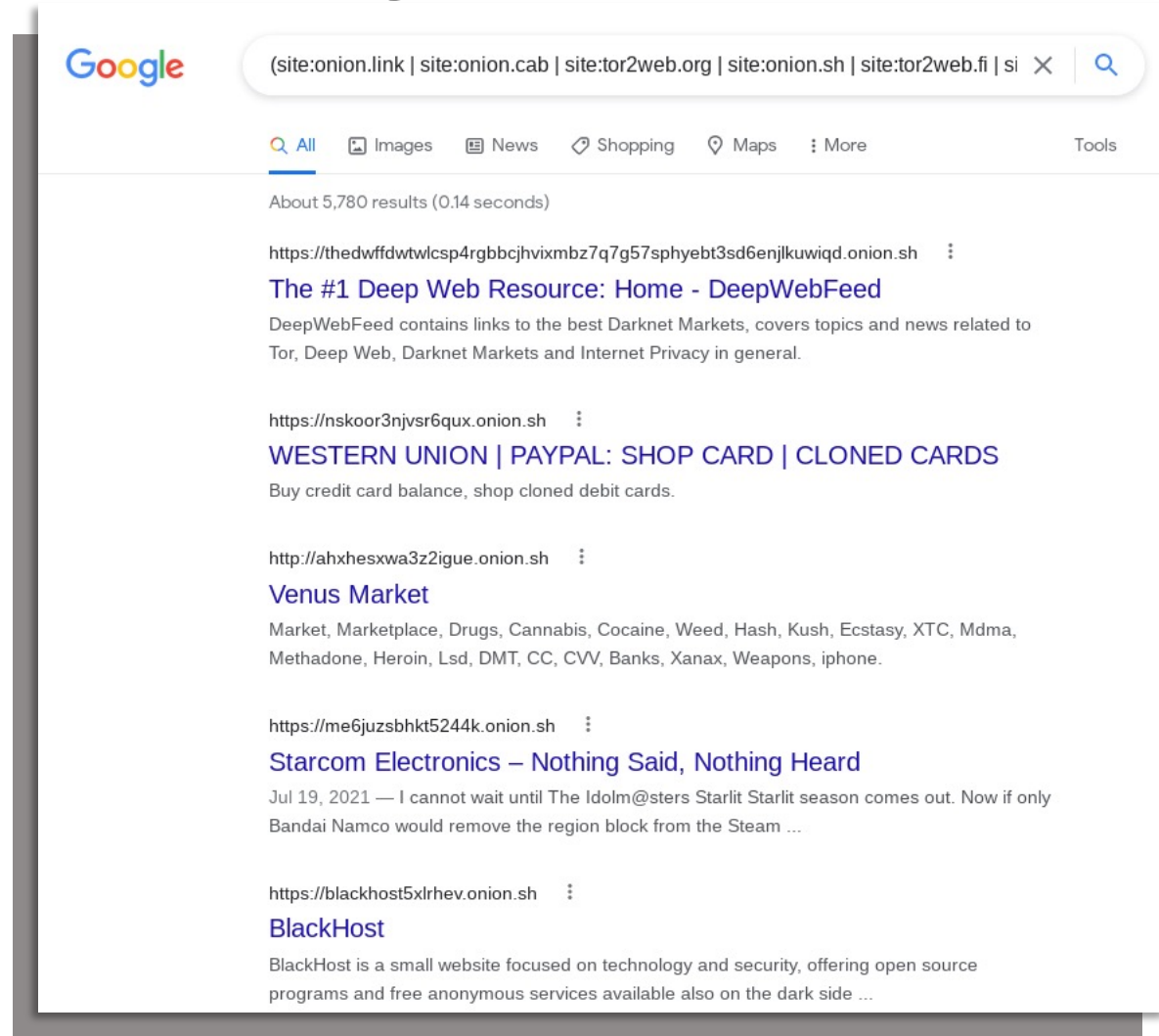
(hxxp:// OR http://)[.] AND url:onion

# Look for sources - Google

- The Google Dork to use is:

(site:onion.ly |  
site:onion.link|  
site:onion.cab|  
site:tor2web.org|  
site:onion.sh |  
site:tor2web.fi|  
site:onion.direct)

#WEINNOVATE



# Look for sources - Telegram

PARENTAL  
ADVISORY  
EXPLICIT CONTENT

## Hidden Links

RANION (RaaS) | FUD Ransomware

<http://qaoxsnp5cjxbv7duyo7e52dvsagxxveq2gm4w5b7vwr3ecpxatonid.onion>

Category: Hacking

//////////

RANION (RaaS) | FUD Ransomware

//////////

348 02:33

## Hidden Links

Brians Club

<http://zccnc6wka3dk7r4a3dpfr635vmartytahfv7xafyhkp7tf2wiownqoyd.onion>

Category: Carding

//////////

BRIAN'S CLUB - BIGGEST SHOP OF FRESH DUMPS & CVV2 CARDS.  
DAILY UPDATE'S

//////////

361 02:33

## Hidden Links

NamasteLSD Private Shop

<http://e5fc3et2gcsvmii4f6mrjgapd22azni6iu6pm54m44awfmohevnnpid.onion>

Category: Catalogue

//////////

Insane deals and new products. Dont miss out on it! [Speed, LSD,  
MDMA, KETA]

//////////

378 02:35

August 28

## Hidden Links



Assassination Network -  
Hitman for Hire

<http://assasfsmkhouysvityuxhzsfgsotsziqqipcca5aaxuluo7w4vfwuid.onion/>

Category: Hitman

//////////

Assassination Network -  
Hitman for Hire

//////////

328 08:44

#WEINNOVATE

# Look for sources – Data Scraping

```
#!/usr/bin/python3

from modules.utilities import queries as q, functions as fun
from datetime import datetime
from bs4 import BeautifulSoup
import requests
import time

tool = "XSS"
fun.ins_up(q.insert_log, tool, int(time.time()), f"START OF {tool}", 1, tool)
print(f'{datetime.now().strftime("%d/%m/%Y %H:%M:%S")} - START {tool}')

thread = 13058
with open('xss_manual.log', 'a') as f:
    while thread < 100000:
        session = requests.session()
        session.proxies = {}

        session.proxies['http'] = 'socks5h://localhost:9050'
        session.proxies['https'] = 'socks5h://localhost:9050'

        url_base = fun.select_one(q.select_link, tool, tool)

        r = session.get(url_base)
        cookies = {}
        for c in r.cookies:
            cookies={c.name: c.value}
        soup = BeautifulSoup(r.text, 'html.parser')
        token = soup.find('input', type='hidden')['value']
        headers = {'Content-Type': 'application/x-www-form-urlencoded'}
        r = session.post(f'{url_base}/login/login', data=f'login={username}&password={password}&remember=1&xfRedirect=&xfToken={token}', cookies=cookies, headers = headers)
        f.write(f'{r.status_code} login\n')
        for tmp in range(3000):
            url_thread = f'{url_base}/threads/{thread}/'
            r = session.get(url_thread, stream=True)
            f.write(f'{r.status_code}, {url_thread}\n')
            if r.status_code == 200:
                soup = BeautifulSoup(r.content, 'html.parser')
                if len(soup.find_all('li', class_='pageNav-page')) > 0:
                    max_page = int(soup.find_all('li', class_='pageNav-page')[-1].find('a').contents[0])
                else:
                    max_page = 1
                for page in range(1,max_page + 1):
                    if page != 1:
                        url_page = f'{url_thread}page-{page}'
```

## Goals:

- automate login to a forum
- browse posts
- interact with them (to unlock content)
- search using keywords

# Look for sources – Cyber Criminals Forum

ramp4u5iz4xx75vmt6nk5xfrs5mrrtokszqxhhjqlk7pbwykaz7zid.onion

RAMP

Все лентыRAMPИнфо и ПОРынокВопросыОфтопАрбитраж

Online

Orange 19 Августа 2021 в 16:31  
Администратор

Cobalt Strike 4.4 (Licensed)

Original/Licensed CS 4.4

Активность: johndoe в 11 Сентября 2021 в 05:33

Online

johndoe 22 Августа 2021 в 08:53  
Пользователь

запатченные валидные 10к fortiNet

личным архивом на усмотрение модератора

Активность: johndoe в 11 Сентября 2021 в 05:27

Info and PO

999

31 Августа 2021 в 06:19  
Модератор

открытие форума! подарки!

в честь открытия форума как и полагается выдаем подарки-а что это за подарки, подумае

Активность: Orange в 11 Сентября 2021 в 04:31

Market -> Donations

999

18 Августа 2021 в 01:10  
Модератор

Новости о Ramp

Параноидальное или PR, сами решайте

Активность: Orange в 11 Сентября 2021 в 04:21

Offtopic

13 онлайн

Не беспокоить

devils

Vishka

14 Сен в 18:05

Отвечить

devils

segvec

http://xingnewj6m4qytjhfwemngm7r7rogrindbq7wrfeepejgxc3bwci7qd.onion/

14 Сен в 18:07

Отвечить

segvec

devils

Ага, этот есть. Но там не списаться с ними, не нашел по крайней мере

14 Сен в 18:15

Отвечить

Vishka

devils

у них сайт упал

14 Сен в 19:26

Отвечить

KAJIT

segvec

пиши че передать хош. передам. они не идут на контакт особо. закрытая группа

15 Сен в 02:21

Отвечить

Mafia

What is your favorite way to disable AV's as a Domain Admin.

15 Сен в 11:24

Отвечить

KAJIT

Mafia

if its hasnt passwords just click on some buttons as DA lol

15 Сен в 11:37

Отвечить

Arbuz00

как дела сучки

15 Сен в 17:05

Отвечить

Arbuz00

Mafia

depends which av

15 Сен в 17:06

Отвечить

Напишите сообщение. Для отправки нажмите Enter

# Interact with cyber criminals



**KAJIT**  
Paid registration

[Follow member](#)

[Message](#)

| CONTENT COUNT | JOINED      | MEMBER ID | LAST VISITED |
|---------------|-------------|-----------|--------------|
| 129           | February 21 | 114359    | 1 hour ago   |



**KAJIT**  
Пользователь  
(L2) cache  
Регистрация: 02.02.2021  
Последняя активность: 18 мин. назад

Сообщения  
369

[Подписаться](#) [+ В игнор](#) [Начать переписку](#) [Найти](#)



**Orange**  
Администратор  
AYESHA PRAKASH VP Global

😊 1

[Написать](#)

Регистрация: 2021-08-15 14:28:48  
Последний онлайн: Скрыто  
Создано публикаций: 15  
Оставленно комментариев: 47  
Ответов на вопросы: 1  
Репутация: 1



**LockBitSupp**  
Seller

[Follow member](#)

[Message](#)

| CONTENT COUNT | JOINED  | MEMBER ID | LAST VISITED |
|---------------|---------|-----------|--------------|
| 30            | March 8 | 114846    | May 20       |



**KAJIT**  
Модератор  
flipping\_bits\_as\_a\_service

😊 1

[Написать](#)

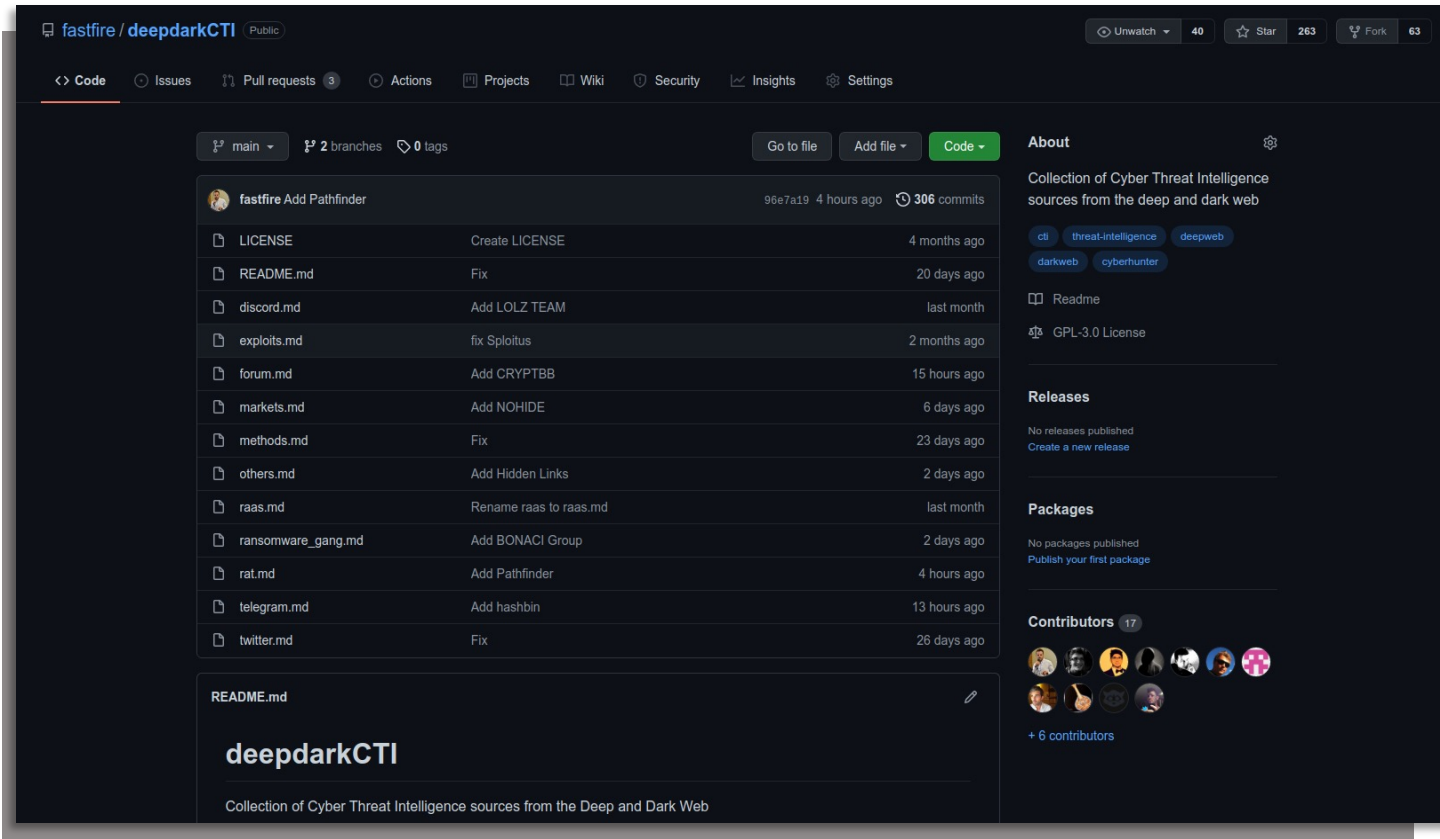
Регистрация: 2021-08-14 17:29:04  
Последний онлайн: Скрыто  
Создано публикаций: 1  
Оставленно комментариев: 15  
Ответов на вопросы: 2  
Репутация: 1

# Look for sources – Recursive research

Look for records found within other sources. In this way you will be able to obtain:

- other useful sources within which to search in the future
- elements that will allow you to enrich the records already found  
(username, email, ip, geographic coordinates, hostnames, domains...)
- other potentially interesting things 😊

# Sources – how to start



deepdarkCTI project  
(<https://github.com/fastfire/deepdarkCTI>)  
→ over 400 sources!

git clone  
<https://github.com/fastfire/deepdarkCTI.git>

make a PR for a new source and join  
Telegram channel!

# Comparison of the web sites

The screenshot shows the Atomsilo Ransomware website. At the top, there is a navigation bar with a 'LIST LEAK' button on the left and the site's name 'Atomsilo Ransomware' in the center, accompanied by a logo of a stylized atom. The main content area is divided into two columns. The left column contains two sections: 'New contacts' with a date 'Sep 18, 00:00' and a message 'Please contact us through the email provided by us.', and 'Updates of data storage rules' with a date 'Sep 18, 00:00' and a message stating that data is stored on servers, recommending ransom payment, and mentioning a blog with 5,000 daily visits. The right column contains two sections: 'Rules' with a list of targets (Hospitals, Critical infrastructure, Oil and gas industry, Educational unit, Non-profit companies) and a statement 'We do not attack:' followed by 'If your company is on that list you can ask us for free decryption.', and 'About us' with a statement 'We are a team that unites people according to one common interest - money.' followed by 'We provide the best service for our clients and partners compared to our competitors.', 'We rely on honesty and transparency in our dealings with our victims.', and 'We never attack the company twice and always fulfill our obligations.'

FOR MEDIA

CONTACT US



LA-Martiniquaise

LA-MARTINIQUAISE.COM

DATA SIZE

30 GB

Data contains:

- Banking
- Details of agreements
- Contracts
- Internal company docs
- Customers files
- Customers Data

PUBLISHED

GO TO POST



BCP Securities

BCPSECURITIES.COM

DATA SIZE

14 GB

Trading operations, brokerage accounts and data.

- Banking
- Details of agreements
- Contracts
- Internal company docs
- Customers files

PUBLISHED

GO TO POST



CasagrandeGroup

CASAGRANDEGROUP.COM

DATA SIZE

11 GB

Data contains:

- Banking
- Details of agreements
- Contracts
- Internal company docs
- Customers files

PUBLISHED

GO TO POST



EQUITY INC

EQUITYINC.INFO

DATA SIZE

200 GB

Data contains:

- Accounting
- HR
- Safety
- Deposits received
- Payroll
- Billing

PUBLISHED

GO TO POST



Actief-Jobmade

ACTIEF-JOBMADE.AT

DATA SIZE

14 GB

Data contains:

- Banking
- Details of agreements
- Contracts
- Internal company docs
- Customers files

PUBLISHED

GO TO POST



Pramer Baustoffe GmbH

PRAMER.AT

DATA SIZE

20 GB

Data contains:

- Banking
- Details of agreements
- Contracts
- Internal company docs
- Customers files

PUBLISHED

GO TO POST

[illegible]

```

14  view-source:http://blackmas7sufmbwtcy3xlozpm356gys34y4rcy/pw/7mifuedyondion/
15
16  <div class="header navbar-expand-md navbar-dark bg-black-25">
17    <div class="navbar-collapse collapse w-100 order-1 order-md-0 dual-collapse2">
18      <div class="navbar-nav mr-auto">
19        <li class="nav-item">
20          <a class="btn btn-outline-light btn-sm" href="/for-media/" for media/a>
21            </li>
22          </div>
23        <div class="nav auto order-0">
24          <a class="navbar-brand mr-auto" href="/">
25            
26            <span class="h1 font-weight-bold" blackletter/>span
27            <span class="h1" "Bannerware">span
28          </div>
29        <div class="navbar-collapse collapse w-100 order-3 dual-collapse2">
30          <div class="navbar-nav mr-auto">
31            <li class="nav-item">
32              <a class="btn btn-outline-light btn-sm" href="/contactmodal/" data-toggle="modal" data-target="#contactmodal">contact us/a>
33            </li>
34          </div>
35        </div>
36      <div id="page">
37
38        <div id="w" class="posts"><div class="container-fluid mt-3"><div class="row"><div class="col-post col-4 mb-3" data-key="7">
39          <div class="card card-post bg-black-25">
40            <div class="card-header p-3">
41              <div class="d-flex">
42                <div style="height: 120px; width: 110px; display: inline-block; class="bg-black-25 text-center">
43                  <div style="display: inline-block; table-cell; text-align: center; vertical-align: middle;">
44                    
45                  </div>
46                <div style="width: calc(100% - 140px); margin-left: 10px; height: 100px; class="">
47                  <div class="text-left">
48                    <h4 class="post-announce-name" title="LA Martiniquaise">LA Martiniquaise/ha
49                  </div>
50                  <div class="text-left">
51                    
52                    <a href="https://www.la martiniquaise.com" class="btn btn-outline-light btn-sm p-1 btn-site" style="border-style: dashed; target: _blank" rel="noopener">
53                      la martiniquaise.com
54                    </a>
55                  </div>
56                <div class="bg-black-25 w-100 mt-3 p-2 text-center">
57                  <div class="bg-white text-weight-bold">
58                    <div class="w-50 border-right">
59                      DATA SIZE
60                    </div>
61                    <div class="w-50">
62                      30 GB
63                    </div>
64                  </div>
65                </div>
66              </div>
67            </div>
68          </div>
69        </div>
70      </div>
71    </div>
72  </div>

```

# Let's analyze the surface!

- **Activate a communication channel:**

```
socat TCP4-LISTEN:8080,reuseaddr,fork  
SOCKS4A:127.0.0.1:qty3gmiq3zhs7whorla4ynvmndppmn5rgcuvsltgz7xl  
6xnxdxtp6zqd.onion:80,socksport=9050
```

- **Perform a scan with nmap:**

```
sudo docker run --rm -it milesrichardson/onion-nmap -p 80,443  
qty3gmiq3zhs7whorla4ynvmndppmn5rgcuvsltgz7xl6xnxdxtp6zqd.onion
```

- **Perform a scan with nikto:**

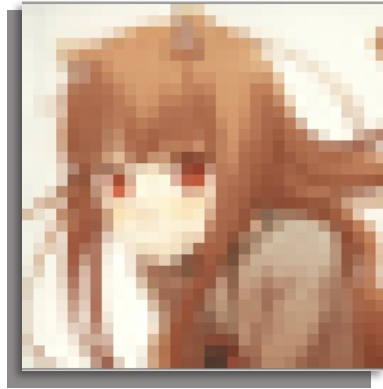
```
nikto -h 127.0.0.1:8080
```

- **Perform a scan with dirb:**

```
dirb http://127.0.0.1:8080 /usr/share/dirb/wordlists/common.txt
```



# Correlation - Favicon



- Get the favicon.ico:  
`wget 127.0.0.1:8080/favicon.ico`
- Calculate md5:  
`md5sum favicon.ico`  
`b2ee4b1225b189eb34a73b833f4cc0c4 favicon.ico`



# Deanonymization - Shodan

109.74.204.67

Regular View Raw Data History

// TAGS: cloud

// LAST UPDATE: 2021-09-26

### General Information

|                |                             |
|----------------|-----------------------------|
| Hostnames      | li151-67.members.linode.com |
| Domains        | LINODE.COM                  |
| Cloud Provider | Linode                      |
| Cloud Region   | gb-eng                      |
| Country        | United Kingdom              |
| City           | London                      |
| Organization   | Linode, LLC                 |
| ISP            | Linode, LLC                 |
| ASN            | AS63949                     |

### Open Ports

|    |    |     |       |
|----|----|-----|-------|
| 21 | 80 | 443 | 10000 |
|----|----|-----|-------|

// 21 / TCP 755911913 | 2021-09-23T03:28:30.427424

```
220 (vsFTPd 3.0.3)
530 Login incorrect.
530 Please login with USER and PASS.
211 Features:
  UTF8
  EPRT
  EPSV
  MDTM
  PASV
  REST STREAM
  SIZE
  TVFS
211 End
```

// 80 / TCP -2077260913 | 2021-09-24T00:00:58.257455

### Apache httpd 2.4.49

```
HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 00:00:56 GMT
Server: Apache/2.4.49 (Ubuntu)
Link: <http://cpctzzh3xzntqwz3.onion/wp-json/>; rel="https://api.w.org/"
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

### Web Technologies

MYSQL PHP WORDPRESS

- The Shodan Dork to use is:  
".onion" !Onion-Location



# Deanonymization - Onionscan

```
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Date:Fri, 17 Sep 2021 16:06:22 GMT (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Etag:W/"6144bcae-7763" (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Buffer Overflow: Favorite Color CTF - OpenPunk (page-info)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 3855969189461981531 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 8934515290638936746 (database-id)
2021/09/17 18:07:00 ERROR: invalid character '\x01' in string literal
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 4611400718388576497 (database-id)
2021/09/17 18:07:00 ERROR: Document '6780609544066090325' does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 6780609544066090325 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 9072649161537808435 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 1837182767186045209 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 4921400023897088956 (database-id)
2021/09/17 18:07:00 ERROR: Document '6728919694038192375' does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 6728919694038192375 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 464585910815582286 (database-id)
2021/09/17 18:07:00 ERROR: Document '6007919213868696143' does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 6007919213868696143 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 3473703075536695017 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 4189801834529524379 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 1381786744247061729 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 3053338413181571919 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 5619774672271116622 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 4911160317317534679 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 8763145465673913453 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 3224922909337500105 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 3957433045648308588 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 2590059260726512071 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 784414512145923700 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 7056359928523774603 (database-id)
2021/09/17 18:07:00 ERROR: Document '552484040957687669' does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 552484040957687669 (database-id)
2021/09/17 18:07:00 ERROR: Document '7646401588845709991' does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 7646401588845709991 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 2512679369391491745 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 8464168621111885627 (database-id)
2021/09/17 18:07:00 ERROR: Document '6358657606451057941' does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 6358657606451057941 (database-id)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Connection:keep-alive (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Content-Type:text/html (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Date:Fri, 17 Sep 2021 16:06:25 GMT (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Etag:W/"6144bcae-7dbf" (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Last-Modified:Fri, 17 Sep 2021 16:05:02 GMT (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Permissions-Policy:interest-cohort=() (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Server:nginx/1.18.0 (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> Manipulating Lua VMs: Hooking lua_gettop - OpenPunk (page-info)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 4254937779146100202 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 4285379889134283913 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 2564960793432640974 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- crawl ---> 2218702919604811966 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- snapshot ---> color@104.131.79.111 (email-address)
2021/09/17 18:07:00 Bad hash table - repair ASAP onionscandb/reRelationships/From/4
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwx5pncj2g2cm26fkocr5uh3omnn4utvspad.onion --- snapshot ---> color@104.131.79.111 (email-address)
```

onionscan search for  
headers, email, ip, server  
status page...

(to scan for v3 services  
remember to fix this issue  
<https://github.com/s-rah/onionscan/issues/162>)



# Deanonymization – Server Status

```
2021/09/17 23:00:41 Updating djikiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net:80 (clearnet-link)
2021/09/17 23:00:41 Updating djikiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net (clearnet-link)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- mod_status ---> 182.59.187.196</td><td>http/1.1 (ip)
2021/09/17 23:00:41 Updating djikiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net:80 (clearnet-link)
2021/09/17 23:00:41 Updating djikiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net (clearnet-link)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- clearnetlink ---> http://httpd.apache.org/docs/2.4/mod/mod_userdir.html (uri)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- clearnetlink ---> https://bugs.launchpad.net/ubuntu/+source/apache2 (uri)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- ssh ---> 8b:53:58:d3:1c:5c:92:4f:a7:58:61:0c:d9:74:39:4e (key-fingerprint)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- ssh ---> SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
                (software-banner)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Last-Modified:Sun, 31 Mar 2019 00:41:39 GMT (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Server:Apache/2.4.46 (Ubuntu) (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Vary:Accept-Encoding (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Accept-Ranges:bytes (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Content-Type:text/html (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Date:Fri, 17 Sep 2021 20:59:46 GMT (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Etag:"2aa6-585592ac2e0e7-gzip" (http-header)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> Apache2 Ubuntu Default Page: It works (page-info)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> 1526509918387121164 (database-id)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> 1122467626640935222 (database-id)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> 1955767765639746762 (database-id)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> 4594266401287931334 (database-id)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> 5404207403099481384 (database-id)
2021/09/17 23:00:41 Inserting djikiri5jiruhxv7u.onion --- crawl ---> 6855277419408228227 (database-id)
----- OnionScan Report -----
Generating Report for: djikiri5jiruhxv7u.onion

High Risk: Apache mod_status is enabled and accessible
            why this is bad: An attacker can gain very valuable information from this internal status page including IP addresses, co-hosted serv
            To fix, disable mod_status or serve it on a different port than the configured hidden service.
```

host pendulum.kzin.johnnyware.net  
pendulum.kzin.johnnyware.net is an alias for  
johnnyware.net.  
johnnyware.net has address 123.243.224.217  
johnnyware.net mail is handled by 10 johnnyware.net.

#WEINNOVATE

Apache Server Status for djikiri5jiruhxv7u.onion (via 127.0.0.1)

Server Version: Apache/2.4.46 (Ubuntu)  
Server MPM: prefork  
Server Built: 2021-06-17T17:09:41

Current Time: Tuesday, 21-Sep-2021 12:17:16 UTC  
Restart Time: Tuesday, 03-Aug-2021 03:56:29 UTC  
Parent Server Config. Generation: 50  
Parent Server MPM Generation: 49  
Server uptime: 49 days 8 hours 20 minutes 47 seconds  
Server load: 1.29 1.38 1.50  
Total accesses: 20501 - Total Traffic: 61.3 MB - Total Duration: 922159  
CPU Usage: u31.26 s106.54 cu6.54 cs8.94 - .0036% CPU load  
.00481 requests/sec - 15 B/second - 3136 B/request - 44.9812 ms/request  
1 requests currently being processed, 7 idle workers

W.....  
.....  
.....

Scoreboard Key:  
"." Waiting for Connection, "s" Starting up, "k" Reading Request,  
"V" Sending Reply, "K" Keepalive (read), "g" DNS Lookup,  
"C" Closing connection, "L" Logging, "e" Gracefully finishing,  
"I" Idle cleanup of worker, "-" Open slot with no current process

| Srv   | PID     | Acc       | M CPU  | SS     | Req  | Dur    | Conn | Child | Slot | Client         | Protocol | VHost                           | Request                              |
|-------|---------|-----------|--------|--------|------|--------|------|-------|------|----------------|----------|---------------------------------|--------------------------------------|
| 0-49  | 2082980 | 0/13/2496 | W 0.01 | 0      | 0    | 34345  | 0.0  | 0.06  | 7.46 | 127.0.0.1      | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /server-status HTTP/1.1          |
| 1-49  | 2237846 | 0/13/2202 | 0.01   | 26     | 1    | 127627 | 0.0  | 0.03  | 6.59 | 127.0.0.1      | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /icons/ubuntu-logo.png HTTP/1.1  |
| 2-49  | 2075595 | 0/36/2385 | 0.02   | 4220   | 0    | 61494  | 0.0  | 0.15  | 7.39 | 176.214.43.170 | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.0                        |
| 3-49  | 2075596 | 0/14/1422 | 0.01   | 3415   | 1    | 109705 | 0.0  | 0.08  | 4.29 | 127.0.0.1      | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.1                        |
| 4-49  | 2075597 | 0/14/1225 | 0.02   | 4384   | 0    | 113896 | 0.0  | 0.07  | 3.94 | 178.159.37.182 | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.0                        |
| 5-49  | 2777528 | 0/1/785   | 0.00   | 2605   | 0    | 68707  | 0.0  | 0.00  | 2.04 | 107.189.14.98  | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.1                        |
| 6-48  | -       | 0/0/660   | 0.00   | 44162  | 1200 | 88074  | 0.0  | 0.00  | 1.83 | 107.189.31.252 | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /config/getuser?index=0 HTTP/1.1 |
| 7-48  | -       | 0/0/303   | 0.00   | 44162  | 588  | 10592  | 0.0  | 0.00  | 0.70 | 66.249.65.55   | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /robots.txt HTTP/1.1             |
| 8-48  | -       | 0/0/220   | 0.00   | 44162  | 877  | 17119  | 0.0  | 0.00  | 0.50 | 66.249.65.57   | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.1                        |
| 9-44  | -       | 0/0/275   | 0.00   | 389835 | 0    | 96     | 0.0  | 0.00  | 0.68 | 127.0.0.1      | http/1.1 | 192.168.122.1:80                | GET /HTTP/1.1                        |
| 10-49 | 2075593 | 0/15/1535 | 0.02   | 2528   | 1    | 108628 | 0.0  | 0.08  | 5.25 | 127.0.0.1      | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.1                        |
| 11-49 | 2075594 | 0/16/1851 | 0.01   | 1358   | 0    | 69089  | 0.0  | 0.06  | 6.08 | 34.219.140.108 | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.1                        |
| 12-44 | -       | 0/0/1018  | 0.00   | 434183 | 0    | 22523  | 0.0  | 0.00  | 3.36 | ::1            | http/1.1 | 192.168.122.1:80                | OPTIONS P HTTP/1.0                   |
| 13-44 | -       | 0/0/116   | 0.00   | 389835 | 0    | 45     | 0.0  | 0.00  | 0.30 | 66.249.65.43   | http/1.1 | 192.168.122.1:80                | GET /HTTP/1.1                        |
| 14-41 | -       | 0/0/195   | 0.00   | 640035 | 0    | 22230  | 0.0  | 0.00  | 0.55 | 127.0.0.1      | http/1.1 | pendulum.kzin.johnnyware.net:80 | GET /HTTP/1.1                        |

|                                                |                                                                                                        |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> IP Address | 123.243.224.217                                                                                        |
| <input checked="" type="checkbox"/> Country    |  Australia [AU] ⓘ |
| <input type="checkbox"/> Region                | New South Wales                                                                                        |
| <input type="checkbox"/> City                  | Ryde                                                                                                   |
| <input type="checkbox"/> Coordinates of City   | -33.816670, 151.100000 (33°49'0"S 151°5'60"E)                                                          |

# Deanononymization – Exif Metadata

```
Info: Found Identities
Items Identified:
xubin99051@gmail.com
yourmail@example.com
//blogswbiobot
you@example.com
horologicalhost
talkgarchlinuxcn.org
-farseerf@archlinux/tu/farseerfc
root@localhost
root@192.168.1.1
room@domain.tld
shadowrz@disroot.org
aletxpol@kde.org
bourigaullfrablang@gmail.com
jonno.conder@gmail.com
aur@aur.archlinux.org
git@github.com
hetnrtch@hugoboss.de
mailaddress@domain.tld
root@192.168.1.1

Medium Risk: Small number of images with EXIF metadata were discovered!
Why this is bad: EXIF metadata can itself deanonymize a user or service operator (e.g. GPS location, Name etc.). Or, when combined, can be used to link anonymous identities together.
To fix, re-encode all images to strip EXIF and other metadata.
Items Identified:
/Images/AOSCC/2019/-1.jpg
/Images/AOSCC/2019/8.jpg
/Images/AOSCC/day2/19.jpg
/Images/AOSCC/2019/4.jpg
/Images/travel_on_hongkong/IMG_20190629_142434.jpg
/Images/playing_dancerush_stardom_chinese/cabinet.jpg
/Images/AOSCC/day1/18.jpg
/Images/AOSCC/2019/18.jpg
/Images/travel_on_hongkong/HVIMG_20190818_185936.jpg
/Images/AOSCC/2019/9.jpg
/Images/AOSCC/day2/3.jpg
/Images/travel_on_hongkong/IMG_0547.jpg
/Images/AOSCC/day2/7.jpg
/Images/AOSCC/2019/0.jpg
/Images/AOSCC/day3/5.jpg
/Images/AOSCC/day1/11.jpg
/Images/travel_on_hongkong/IMG_20190818_185147.jpg
/Images/travel_on_hongkong/IMG_20190622_135809.jpg
/Images/travel_on_hongkong/IMG_20190709_221225.jpg
/Images/AOSCC/day3/10.jpg
/Images/travel_on_hongkong/IMG_20190818_104138.jpg
/Images/travel_on_hongkong/IMG_20190811_133029.jpg
/Images/AOSCC/day3/21.jpg
```

Device Manufacturer : Google  
Device Model :  
Device Attributes : Reflective, Glossy, Positive, Color  
Rendering Intent : Perceptual  
Connection Space Illuminant : D50 Illuminant  
Profile Creator : Google  
Profile ID : 75e1a013c3437a318c8ab60632a28a  
Profile Description : sRGB IEC61966-2.1  
Profile Copyright : Copyright (c) 2016 Google Inc.  
Media White Point : 0.9545 1 1.0895  
Media Black Point : 0 0 0  
Red Matrix Column : 0.43684 0.22249 0.01392  
Green Matrix Column : 0.38512 0.7169 0.0976  
Blue Matrix Column : 0.14355 0.8661 0.71391  
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)  
Chromatic Adaptation : 1.49788 0.92202 -0.45519 0.62959 0.99446 -0.01704 -0.09922 0.01589 0  
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)  
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)  
Image Width : 4032  
Image Height : 3024  
Encoding Process : Baseline DCT, Huffman coding  
Bits Per Sample : 8  
Color Components : 3  
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)  
Aperture : 1.8  
Image Size : 4832x3024  
Megapixels : 12.2  
Scale Factor To 35 mm Equivalent : 0.1  
Shutter Speed : 1/125  
Create Date : 2019:08:18 18:51:47.546037+08:00  
Date/Time Original : 2019:08:18 18:51:47.546037+08:00  
Modify Date : 2019:08:18 18:51:47.546037+08:00  
Thumbnail Image : (Binary data 6000 bytes, use -b option to extract)  
GPS Altitude : 4.6 m Above Sea Level  
GPS Date/Time : 2019:08:18 10:46:48Z  
GPS Latitude : 22 deg 19' 5" N  
GPS Longitude : 114 deg 9' 36.81" E

Jeffrey Friel's Image Metadata Viewer  
(How to use)

Some of my other stuff  
My Blog - Lightroom plugin - Pottery Photos  
"Photo Tack"

URL:   
or  
File:     
☐ Non sano un robot

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal](#), or perhaps an Amazon gift certificate (to: jfr1@frybox.com), or perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the FAQ.

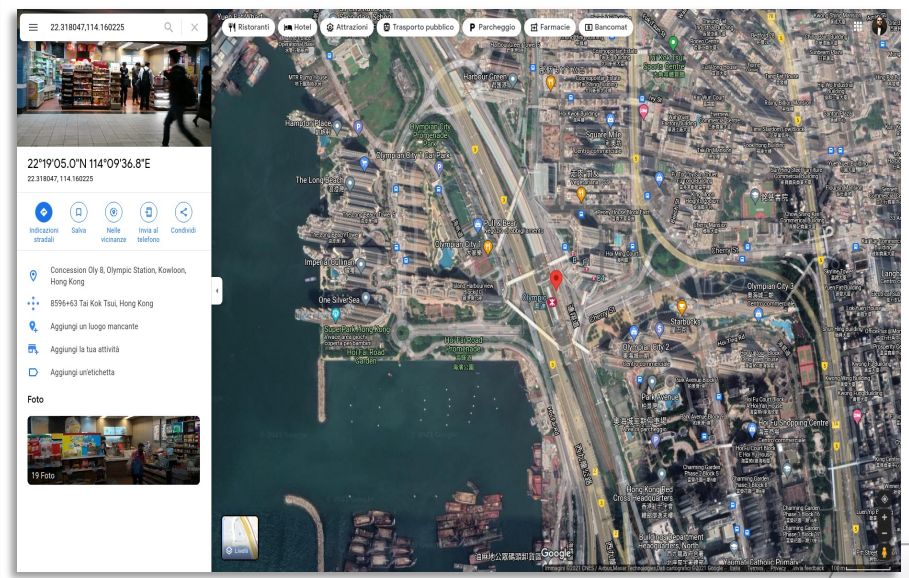
**Basic Image Information**  
Target file: IMG\_20190818\_185147.jpg

**Camera:** Google Pixel 2  
**Lens:** 4.4 mm (Max aperture f/1.8 (shot wide open))  
**Exposure:** Auto exposure, Program AE, 1/125 sec, F1.8, ISO 52  
**Flash:** Off, Did not fire  
**Focus:** At 1.0m, with a depth of field of about 11m. (from about 14cm before the focus point to about 10m after)  
**Date:** August 18, 2019 4:51:47PM (timezone not specified) (2:00h, 30 days, 19 hours, 32 minutes, 33 seconds ago, assuming image timezone of 8 hours ahead of GMT)  
**Location:** Latitude/longitude: 22° 19' 5" North, 114° 9' 36.8" East (22.318047, 114.160225)  
Map via embedded coordinates at: Google, Yahoo, Wikipedia, OpenStreetMap, Bing (also see the Google Maps pane below)  
Altitude: 5 meters (15 feet)  
Camera Pointing: East  
Thumbnail given from earth.google 8 hours ahead of GMT  
**File:** 4.032 x 3.024 JPEG (12.2 megapixels) 2,908,843 bytes (2.8 megabytes)  
**Color Encoding:** Embedded color profile: "sRGB"

Here's the full data:  
**EXIF**

Extracted 255 x 189 0.5-kilobyte "EXIF-Thumbnail Image" JPG  
Displayed here at 100% (1x the area of the original)

Main JPG image displayed here at 11% width (1/9 the area of the original)



#WEINNOVATE

# Cybercrime prevention

**USER:PASS Fortinet SSL VPN FULL 50k INTRANET login**  
by pegg443 - May 09, 2021 at 10:36 PM

Pages (19): 1 2 3 4 5 ... 19 Next »

**pegg443**  
New User  
MEMBER  
Posts: 32  
Threads: 1  
Joined: Mar 2021  
Reputation: 0

May 09, 2021 at 10:36 PM

in 2019, a vulnerability was discovered in Fortinet SSL VPN webpage login (CVE-2018-13379), which could allow unauthenticated users to read a configuration file which contained credentials in plaintext for access to many corporate intranets like the NSA.

this file contains data from 50k hosts, 30k of which contain credentials for accessing the Fortigate SSL VPN for each intranet and potentially giving you access to internal servers and resources.

The size of the uncompressed file is 6.7GB

**Fortinet SSL VPN 50k link**

[https://anonfiles.com/L4uevfveue/FortiFU...13379\\_rar](https://anonfiles.com/L4uevfveue/FortiFU...13379_rar)  
password: xRG666@d1ck#31337

PM Find

Reply Quote Report

## CVE-2021-22893 I buy \$30000+

penilext · 06.05.2021



penilext

пользователь

Регистрация: 02.05.2021  
Сообщения: 2  
Реакции: 1

06.05.2021

Hi. Is anyone able to sell PoC for pulse vpn CVE-2021-22893  
my budget is \$25000+  
write me if you sell

Жалоба



SanctumSemptra

RAID-массив

Пользователь

Регистрация: 05.10.2020  
Сообщения: 77  
Реакции: 13

07.05.2021

Куплю готовый эксплоит CVE-2021-22893  
бюджет 100к\$  
с гарантиями данного форума или соседнего борда

Жалоба

# Is it really possible to prevent (cyber) crime? What do we have available?

## INITIAL ACCESS:

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Supply Chain Compromise
- Phishing
- Valid Accounts
- Trusted Relationship
- Hardware Additions
- Replication Through Removable Media





info@wuerth-phoenix.com  
www.wuerth-phoenix.com



Thank you  
Grazie Danke

#WEINNOVATE