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

Dark Web

Intentionally hidden content.

Can be accessed with special software.

1-4% of the entire internet

Deep Web

Unindexed content (96-99% entire internet).

Cannot be found with traditional search engines.

Networks

friend-to-friend, Tor, Freenet,

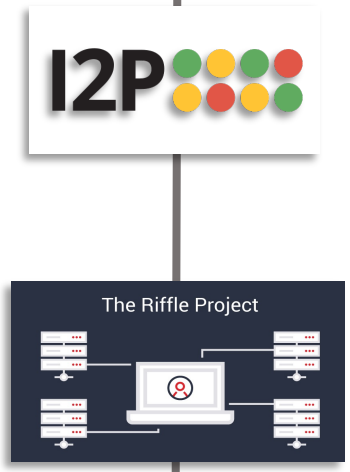
I2P, Riffle, Netsukuku

- https://www.csoonline.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

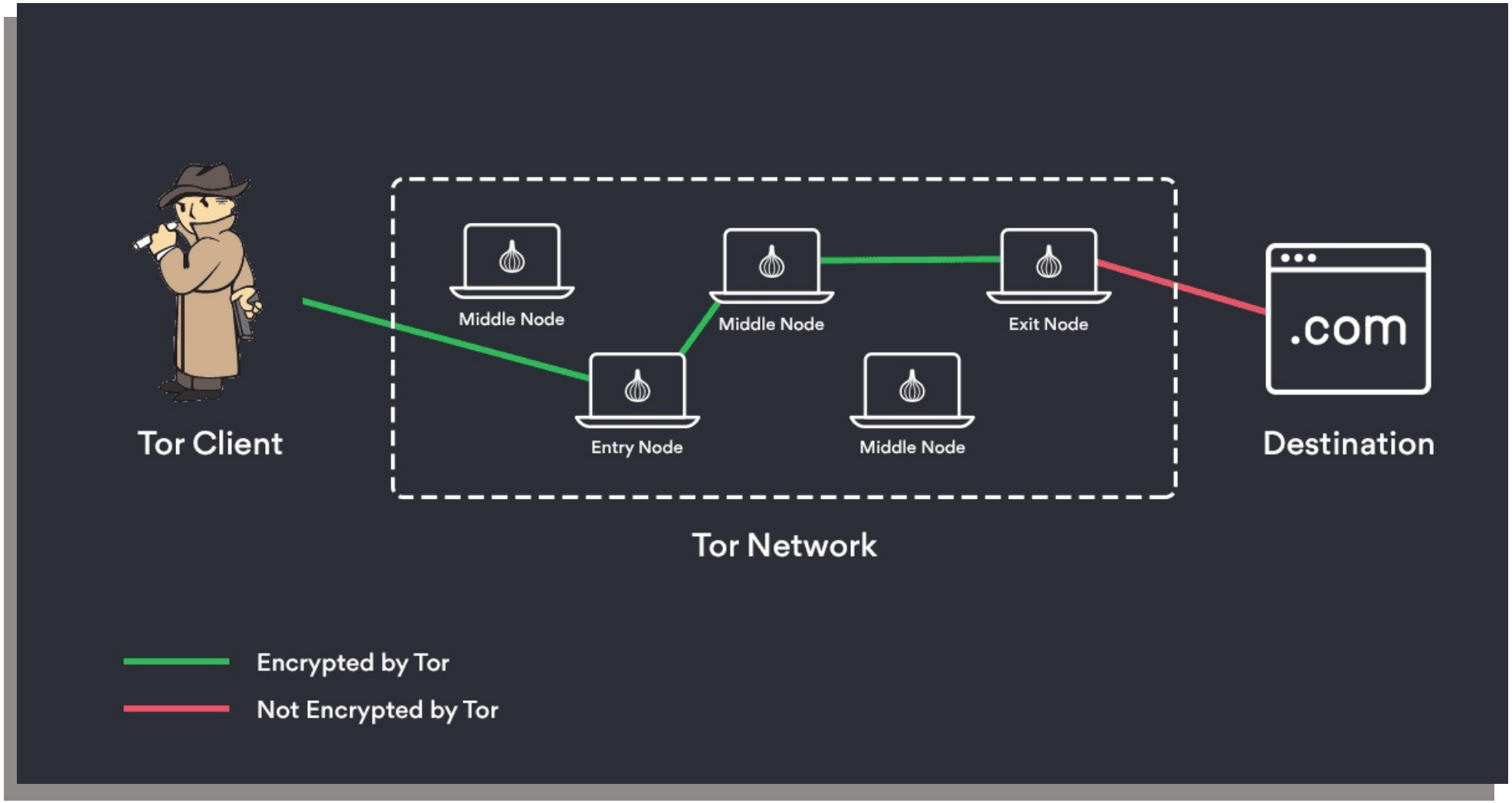
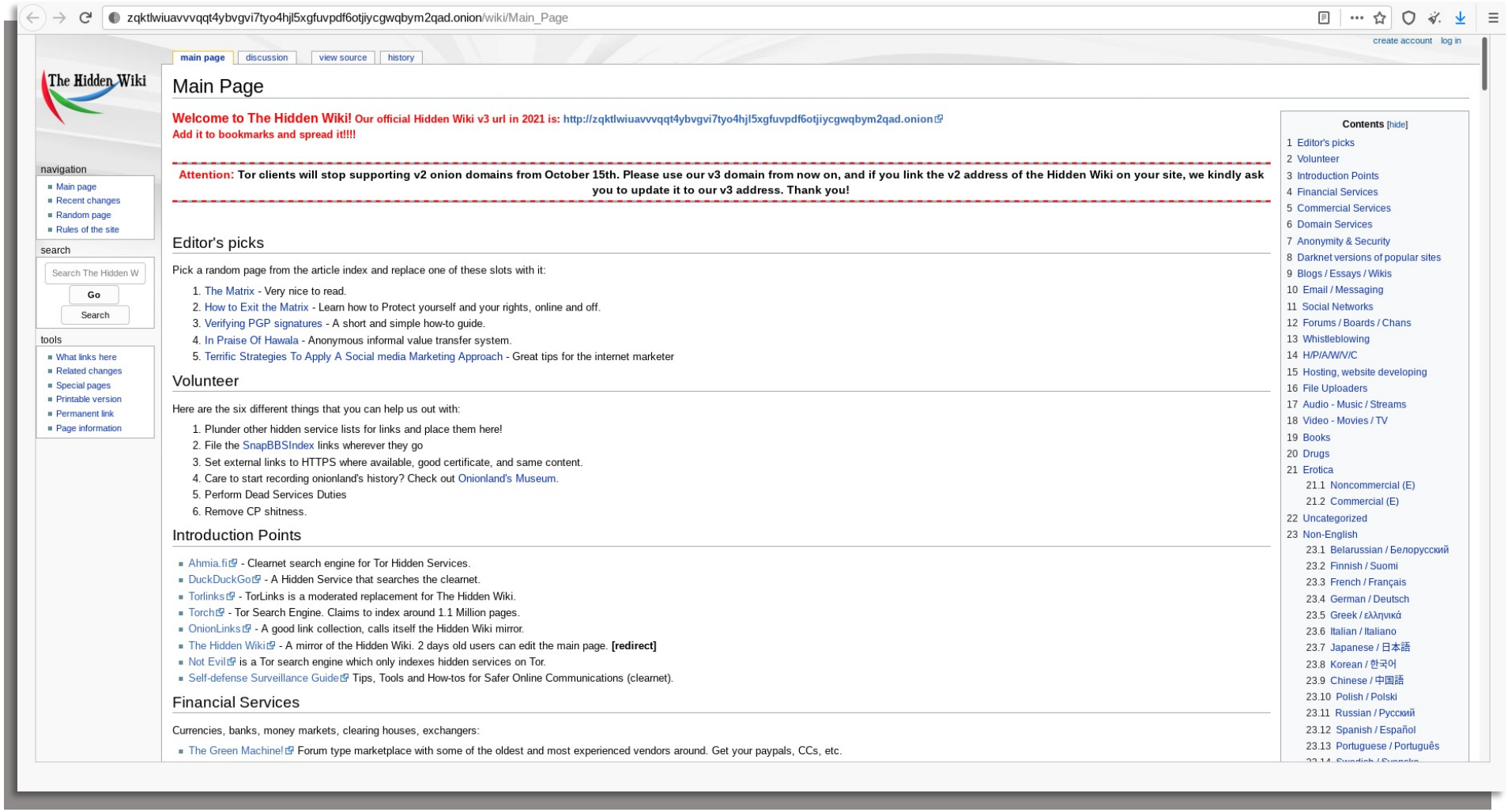


Image from: https://ourcodeworld.com/articles/read/953/how-to-route-all-the-machine-traffic-through-tor-in-kali-linux

Look for sources – hidden services directories



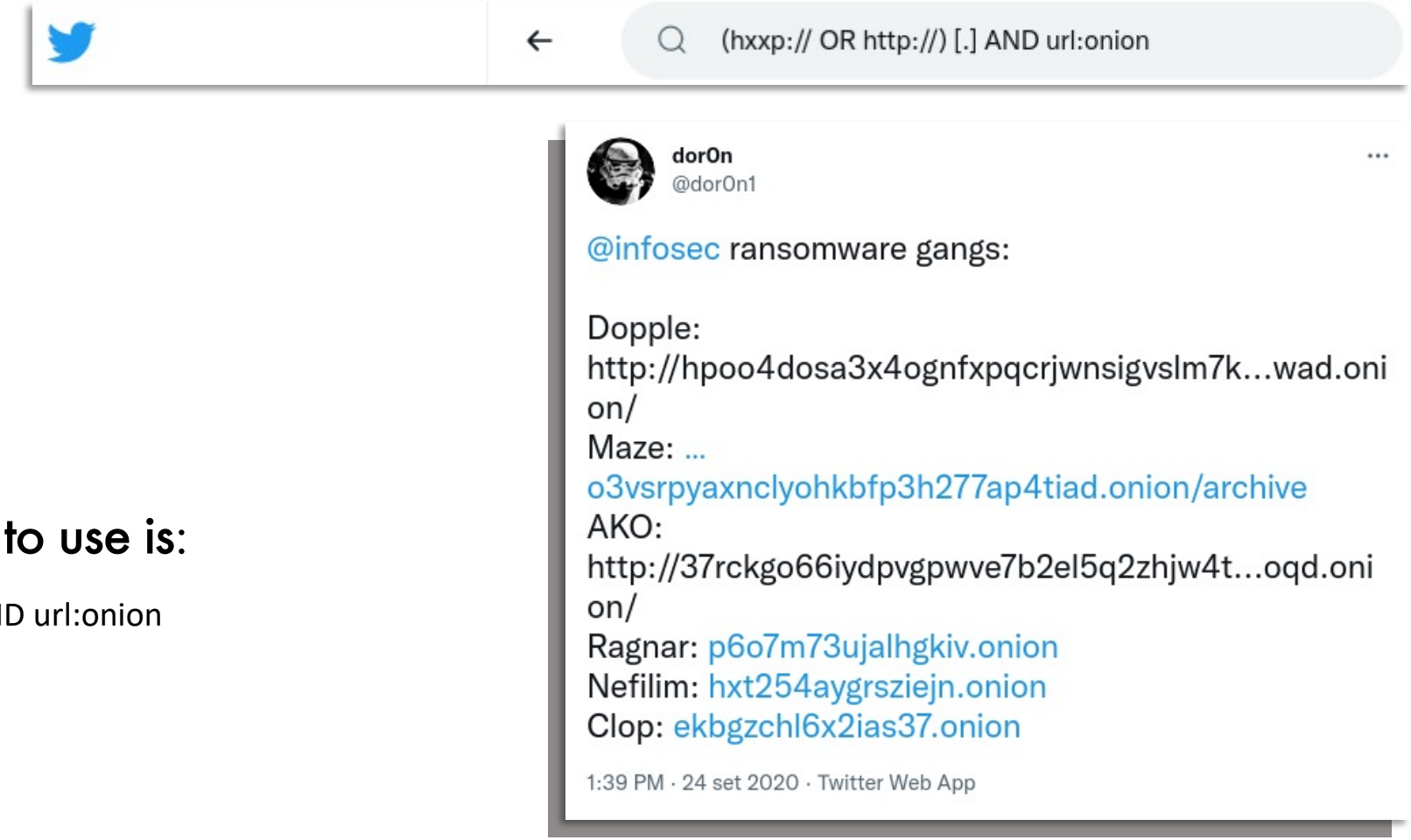
#WEINNOVATE

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/Main_Page

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|

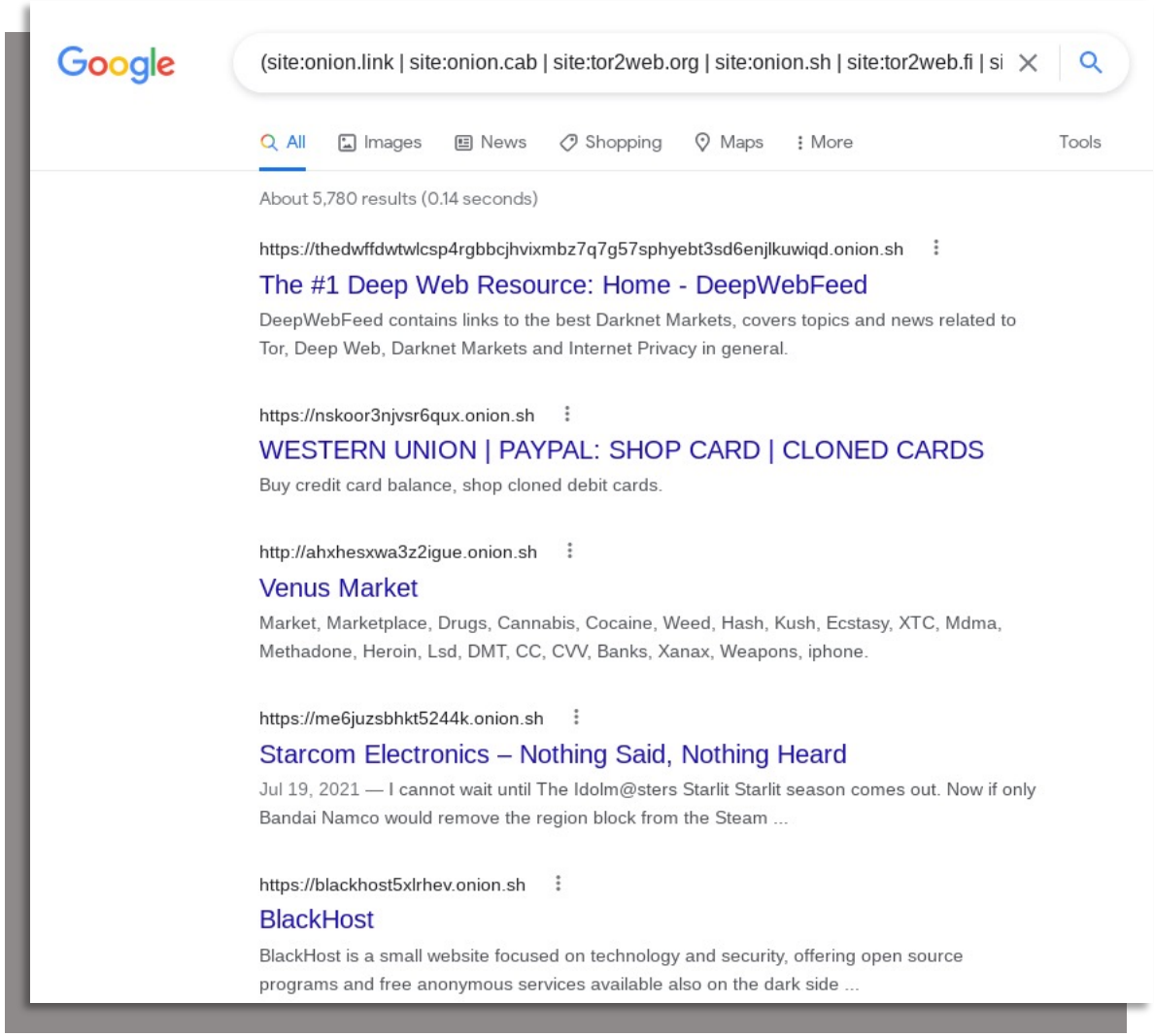
site:onion.cab|

site:tor2web.org|

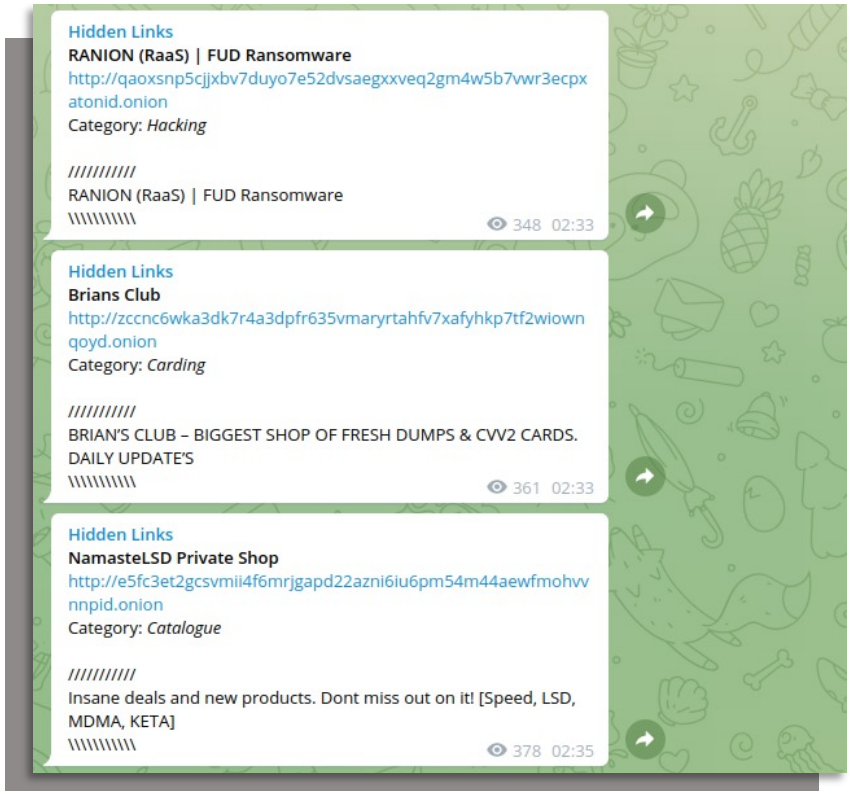
site:onion.sh |

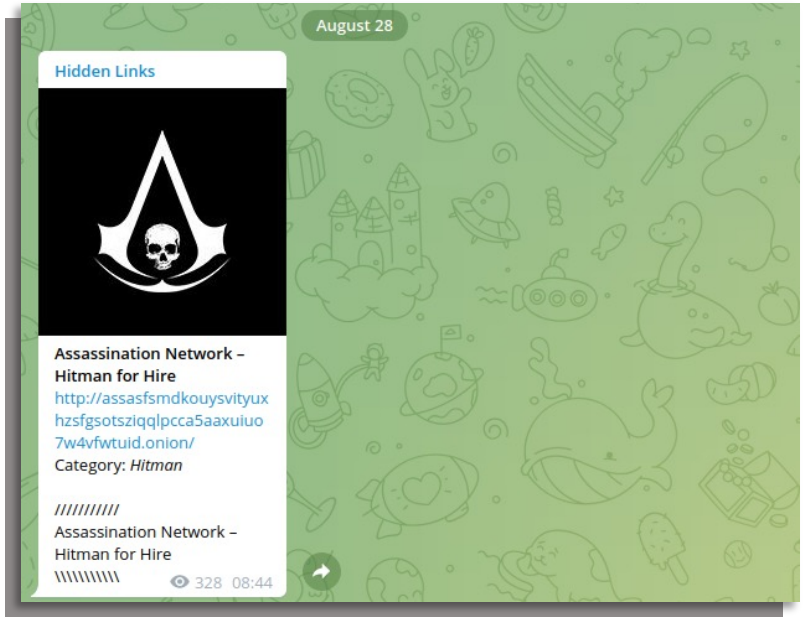
site:tor2web.fi|

site:onion.direct)



Look for sources - Telegram





#WEINNOVATE

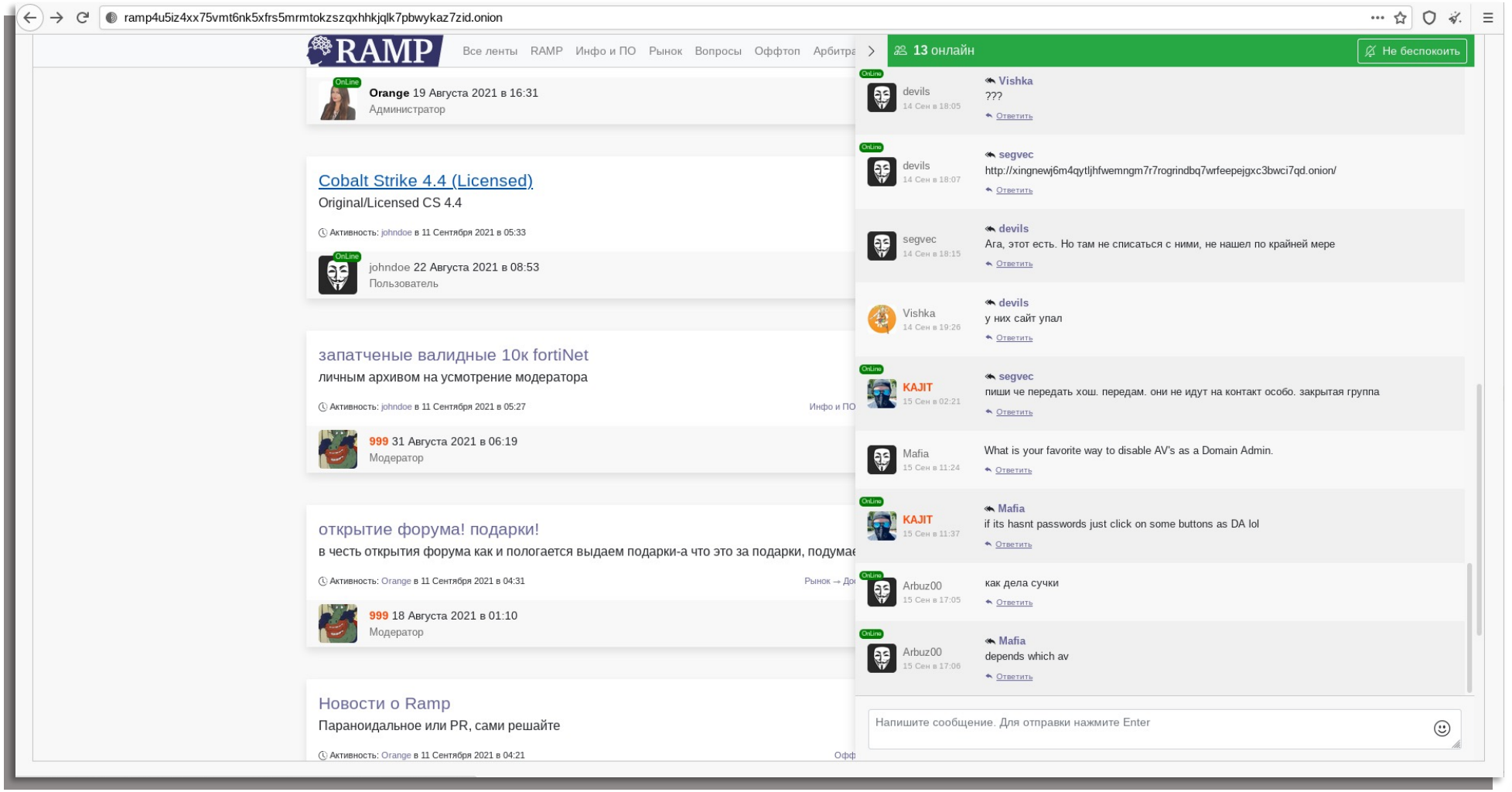
Look for sources – Data Scraping

```python
#!/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=[redacted]&password=[redacted]&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

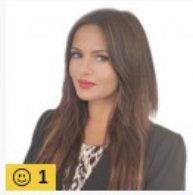


Interact with cyber criminals

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

#WEINNOVATE

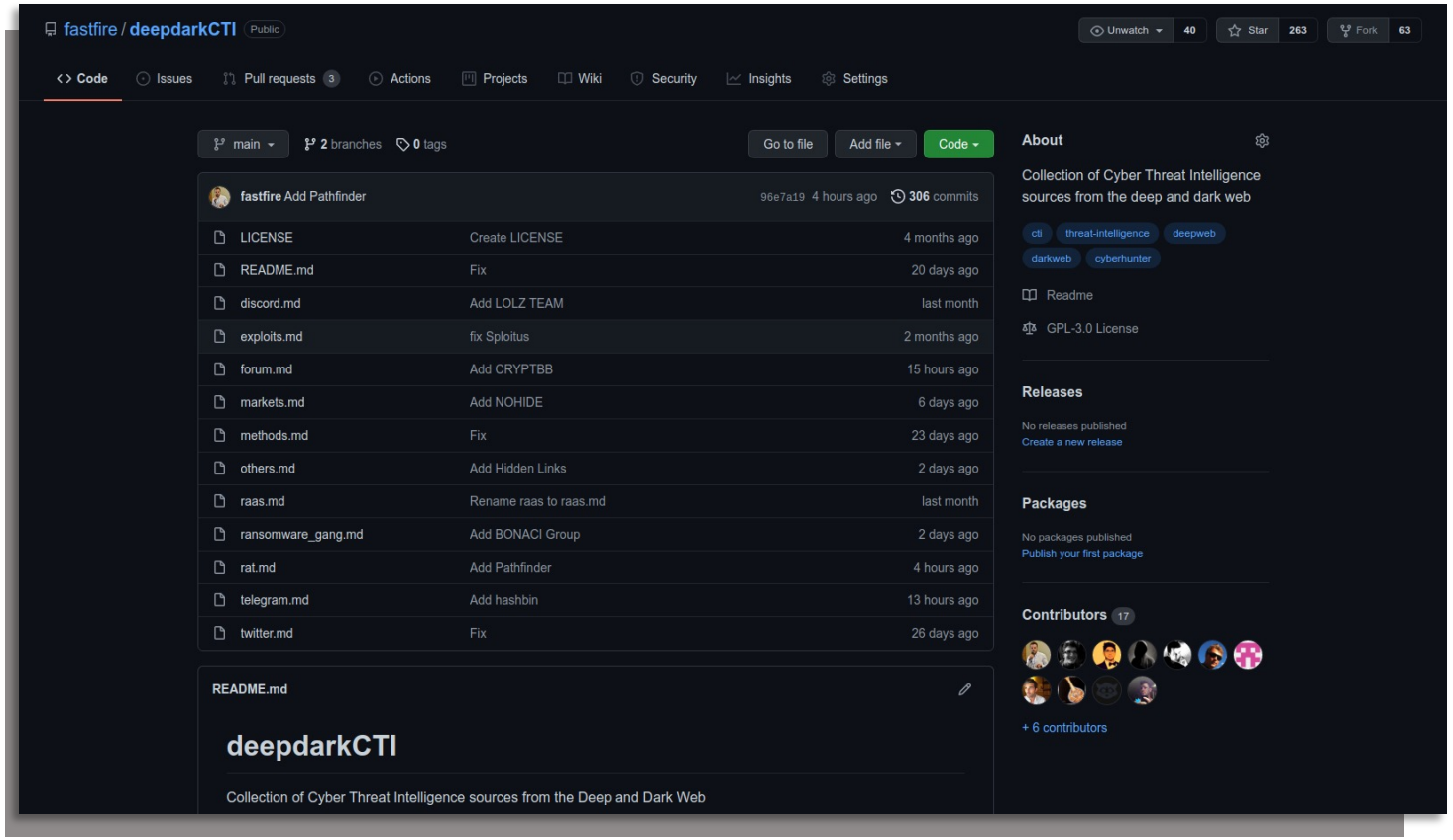
Look for sources – Recursive research

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

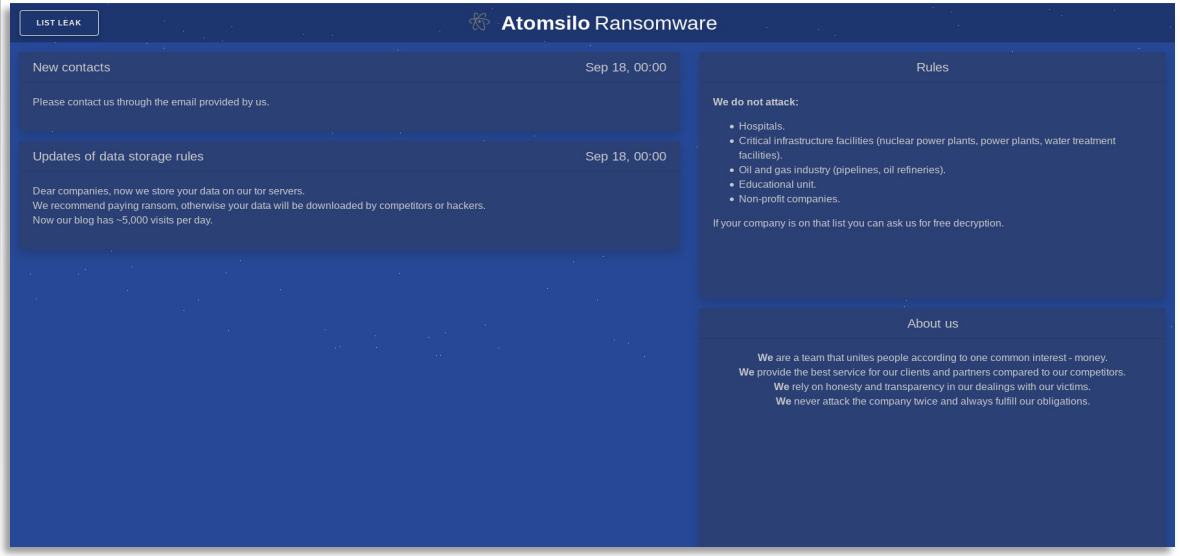


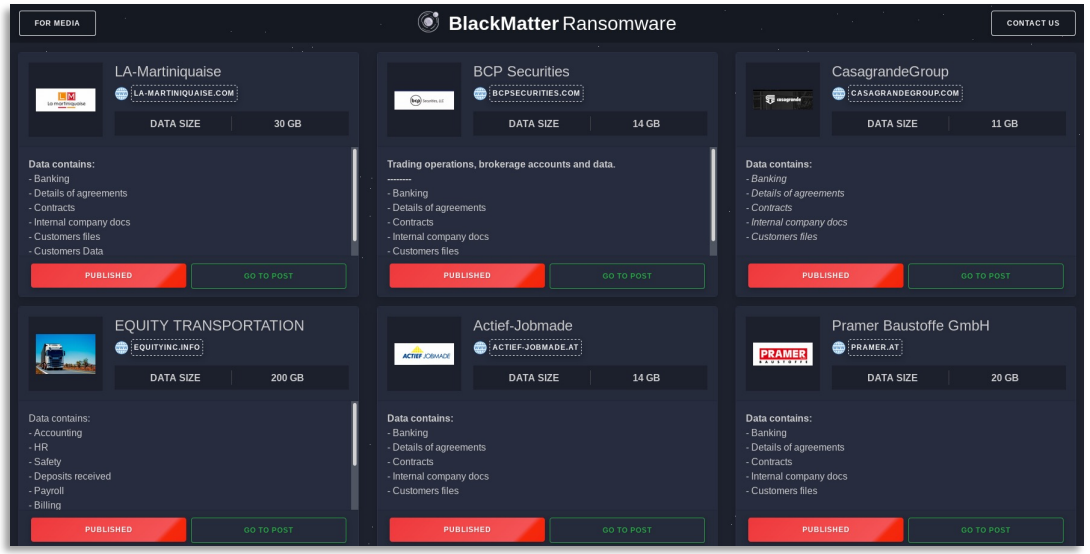
deepdarkCTI project (https://github.com/fastfire/deepdarkCTI)
→ over 400 sources!

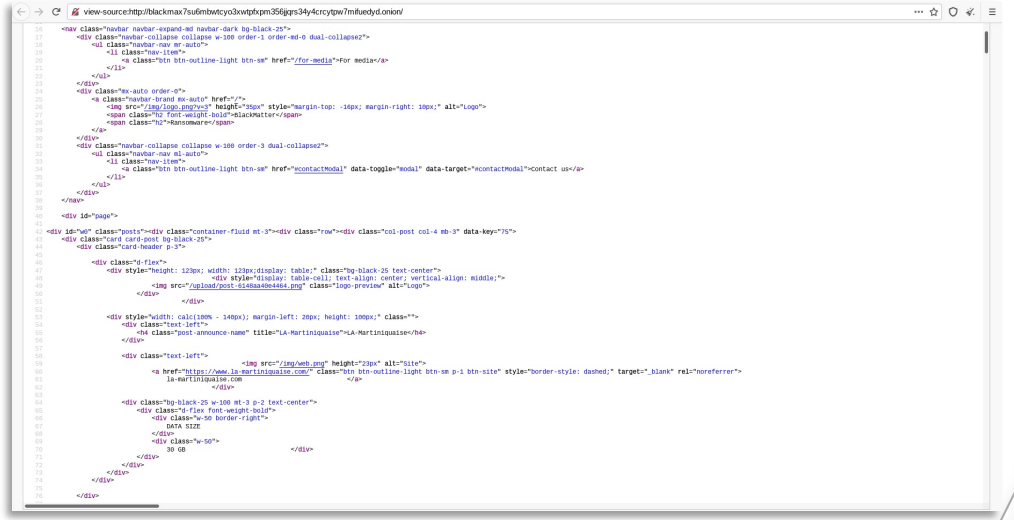
git clone
https://github.com/fastfire/deepdarkCTI.git

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

Comparison of the web sites







Let’s analyze the surface!

- Activate a communication channel:

  socat TCP4-LISTEN:8080,reuseaddr,fork SOCKS4A:127.0.0.1:qty3gmiq3zhs7whorla4ynvmndppmn5rgcuvsltgz7xl6xnxdxtp6zqd.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

Target Site: qty3gmiq3zhs7whorla4ynvmndppmn5rgcuvsltgz7xl6xnxdxtp6zqd.onion

Correlation - Favicon

- Get the favicon.ico:

  wget 127.0.0.1:8080/favicon.ico

- Calculate md5:

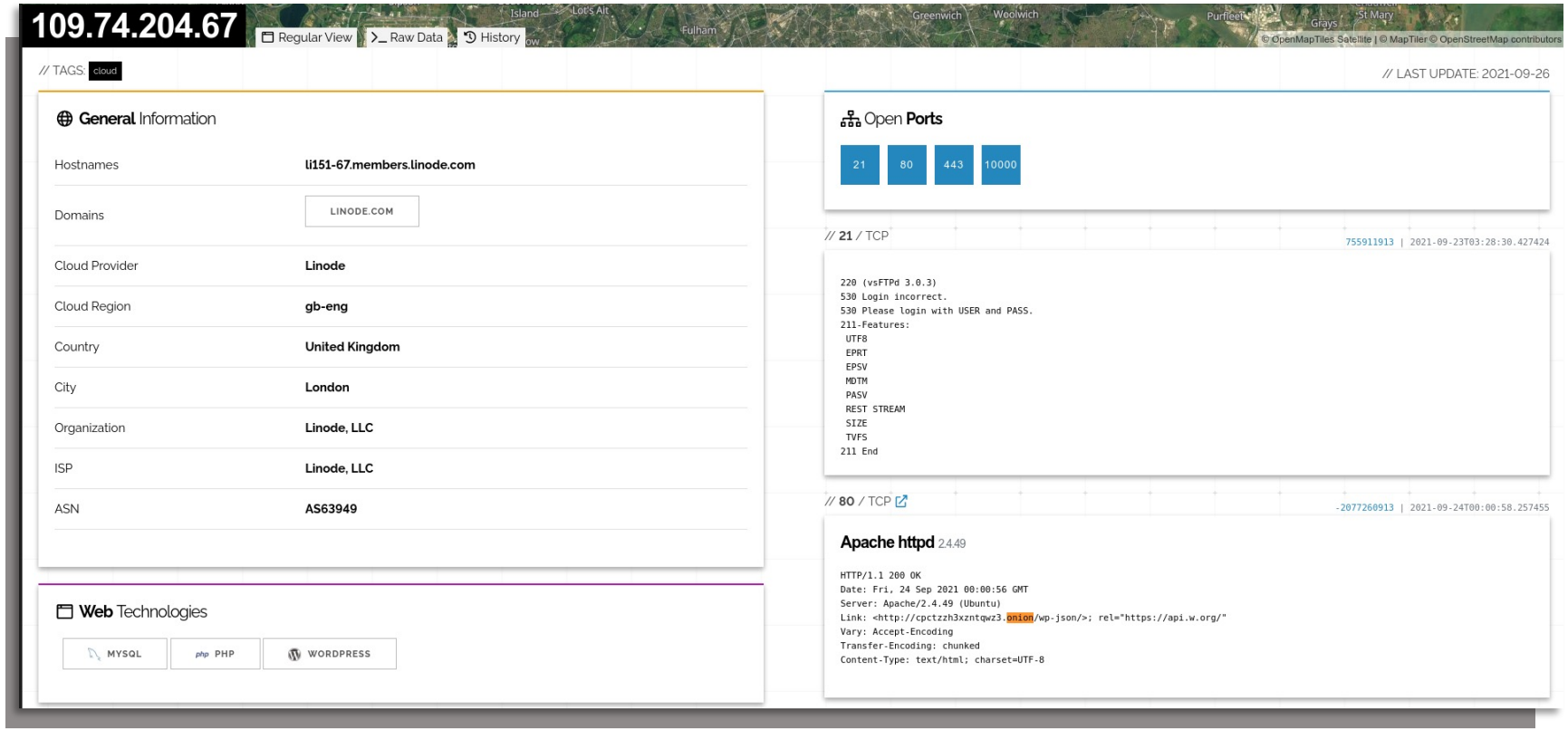
  md5sum favicon.ico

  b2ee4b1225b189eb34a73b833f4cc0c4 favicon.ico

#WEINNOVATE

Target Site: qty3gmiq3zhs7whorla4ynvmndppmn5rgcuvsltgz7xl6xnxdxtp6zqd.onion

Deanonymization - Shodan



- The Shodan Dork to use is:

  ".onion" !Onion-Location

Deanonymization - Onionscan

```
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Date:Fri, 17 Sep 2021 16:06:22 GMT (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Etag:W/"6144bcae-7763" (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Buffer Overflow: Favorite Color CTF - OpenPunk (page-info)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 3855969189461981531 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.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 opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 4611400718388576497 (database-id)
2021/09/17 18:07:00 ERROR: Document `6780609544066090325` does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 6780609544066090325 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 9072649161537808435 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 1837182767186045209 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 4921400023897088956 (database-id)
2021/09/17 18:07:00 ERROR: Document `6728919694038192375` does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 6728919694038192375 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 464585910815582286 (database-id)
2021/09/17 18:07:00 ERROR: Document `6007919213868696143` does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 6007919213868696143 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 3473703075536695017 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 4189801834529524379 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 1381786744247061729 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 3053338413181571919 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 5619774672271116622 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 4911160317317534679 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 8763145465673913453 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 3224922909337500105 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 3957433045648308588 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 2590059260726512071 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 784414512145923700 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 7056359928523774603 (database-id)
2021/09/17 18:07:00 ERROR: Document `5524840409576876669` does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 552484040957687669 (database-id)
2021/09/17 18:07:00 ERROR: Document `7646401588845709991` does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 7646401588845709991 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 2512679369391491745 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 8464168621111885627 (database-id)
2021/09/17 18:07:00 ERROR: Document `6358657606451057941` does not exist
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 6358657606451057941 (database-id)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Connection:keep-alive (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Content-Type:text/html (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Date:Fri, 17 Sep 2021 16:06:25 GMT (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Etag:W/"6144bcae-7dbf" (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Last-Modified:Fri, 17 Sep 2021 16:05:02 GMT (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Permissions-Policy:interest-cohort=() (http-header)
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Server:nginx/1.18.0 (http-header)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> Manipulating Embedded Lua VMs: Hooking lua_gettop - OpenPunk (page-info)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 4254937779146100202 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 4285379889134283913 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 2564960793432640974 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- crawl ---> 2218702919604811966 (database-id)
2021/09/17 18:07:00 Inserting opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- snapshot ---> color@104.131.79.111 (email-address)
2021/09/17 18:07:00 Bad hash table - repair ASAP onionscandb/relationships/From/4
2021/09/17 18:07:00 Updating opnpnk6eutjiqy4ndpyvwxd5pncj2g2cmz6fkocr5uh3omnn4utvspad.onion --- snapshot ---> color@104.131.79.111 (email-address)
```

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

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

https://github.com/s-rah/onionscan

Deanonymization – Server Status

```
2021/09/17 23:00:41 Updating djkiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net:80 (clearnet-link)
2021/09/17 23:00:41 Updating djkiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net (clearnet-link)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- mod_status ---> 182.59.187.196</td><td>http/1.1 (ip)
2021/09/17 23:00:41 Updating djkiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net:80 (clearnet-link)
2021/09/17 23:00:41 Updating djkiri5jiruhxv7u.onion --- mod_status ---> pendulum.kzin.johnnyware.net (clearnet-link)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- clearnetlink ---> http://httpd.apache.org/docs/2.4/mod/mod_userdir.html (uri)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- clearnetlink ---> https://bugs.launchpad.net/ubuntu/+source/apache2 (uri)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.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 djkiri5jiruhxv7u.onion --- ssh ---> SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
 (software-banner)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Last-Modified:Sun, 31 Mar 2019 00:41:39 GMT (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Server:Apache/2.4.46 (Ubuntu) (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Vary:Accept-Encoding (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Accept-Ranges:bytes (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Content-Type:text/html (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Date:Fri, 17 Sep 2021 20:59:46 GMT (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Etag:"2aa6-585592ac2e0e7-gzip" (http-header)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> Apache2 Ubuntu Default Page: It works (page-info)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> 1526509918387121164 (database-id)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> 1122467626640935222 (database-id)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> 1955767765639746762 (database-id)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> 4594266401287931334 (database-id)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> 5404207403099481384 (database-id)
2021/09/17 23:00:41 Inserting djkiri5jiruhxv7u.onion --- crawl ---> 6855277419408228227 (database-id)
--------------- OnionScan Report ---------------
Generating Report for: djkiri5jiruhxv7u.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.
```

djkiri5jiruhxv7u.onion/server-status

Apache Server Status for djkiri5jiruhxv7u.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, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" 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 * 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	-	0/0/185	.	0.00	649035	0	22239	0.0	0.00	0.55	127.0.0.1	http/1.1	pendulum.kzin.johnnyware.net:80	GET / HTTP/1.1

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.

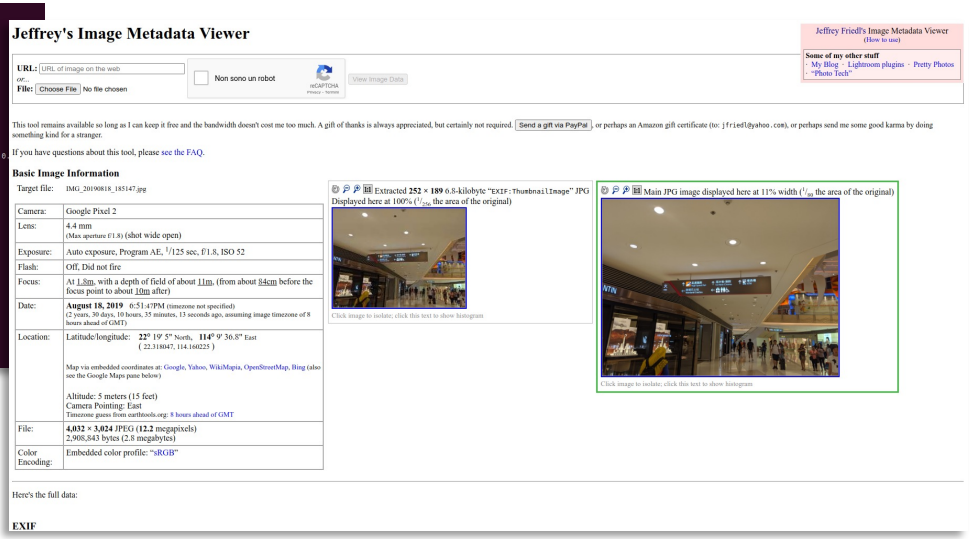
IP Address	123.243.224.217
Country	Australia [AU]
Region	New South Wales
City	Ryde
Coordinates of City	-33.816670, 151.100000 (33°49'0"S 151°5'60"E)

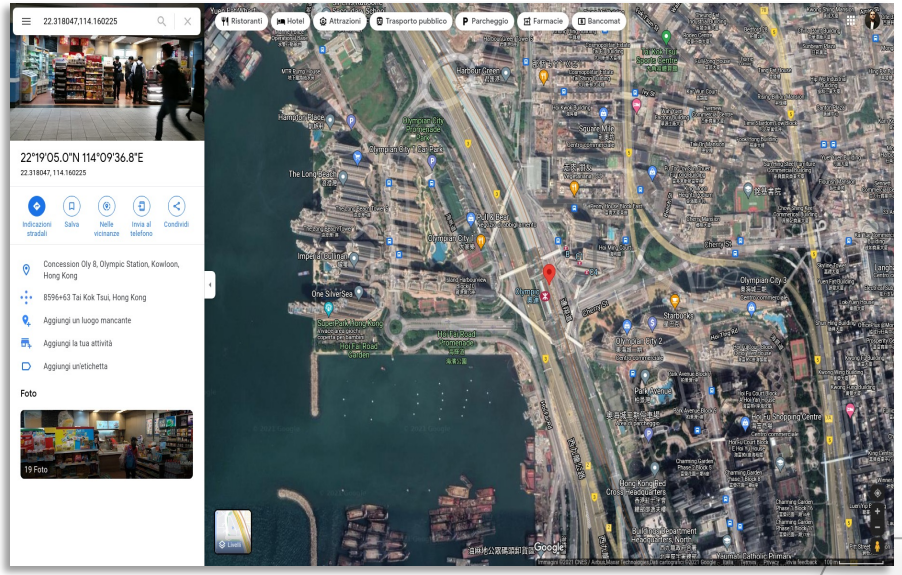
#WEINNOVATE

Deanonymization – Exif Metadata

```
Info: Found Identities
        Items Identified:

        xubin990510@gmail.com
        youremail@example.com
        ///bio@swblobot
        you@example.com
        horo@localhost
        talk@archlinuxcn.org
        ~farseerfc@archlinux/tu/farseerfc
        root@localhost
        root@192.168.1.1
        room@domain.tld
        shadowrz@disroot.org
        alelxpol@kde.org
        bourigaultfabien@gmail.com
        jonno.conder@gmail.com
        aur@aur.archlinux.org
        git@github.com
        heinrichh@duesseldorf.de
        malladdress@domain.tld
        root@192.168

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/MVIMG_20190818_185936.jpg
        /images/AOSCC/2019/9.jpg
        /images/AOSCC/Day3/3.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/Day1/1.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     : 0.9642 1 0.82491
Profile Creator                 : Google
Profile ID                      : 75e1ab013c34376310c8ab660632a28a
Profile Description             : sRGB IEC61966-2.1
Profile Copyright               : Copyright (c) 2016 Google Inc.
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43604 0.22249 0.01392
Green Matrix Column             : 0.38512 0.7169 0.09706
Blue Matrix Column              : 0.14305 0.06061 0.71391
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation            : 1.04788 0.02292 -0.05019 0.02959 0.99048 -0.01704 -0.00922 0.01508 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                      : 4032x3024
Megapixels                      : 12.2
Scale Factor To 35 mm Equivalent: 6.1
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 6988 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' 4.97" N
GPS Longitude                   : 114 deg 9' 36.81" E
```

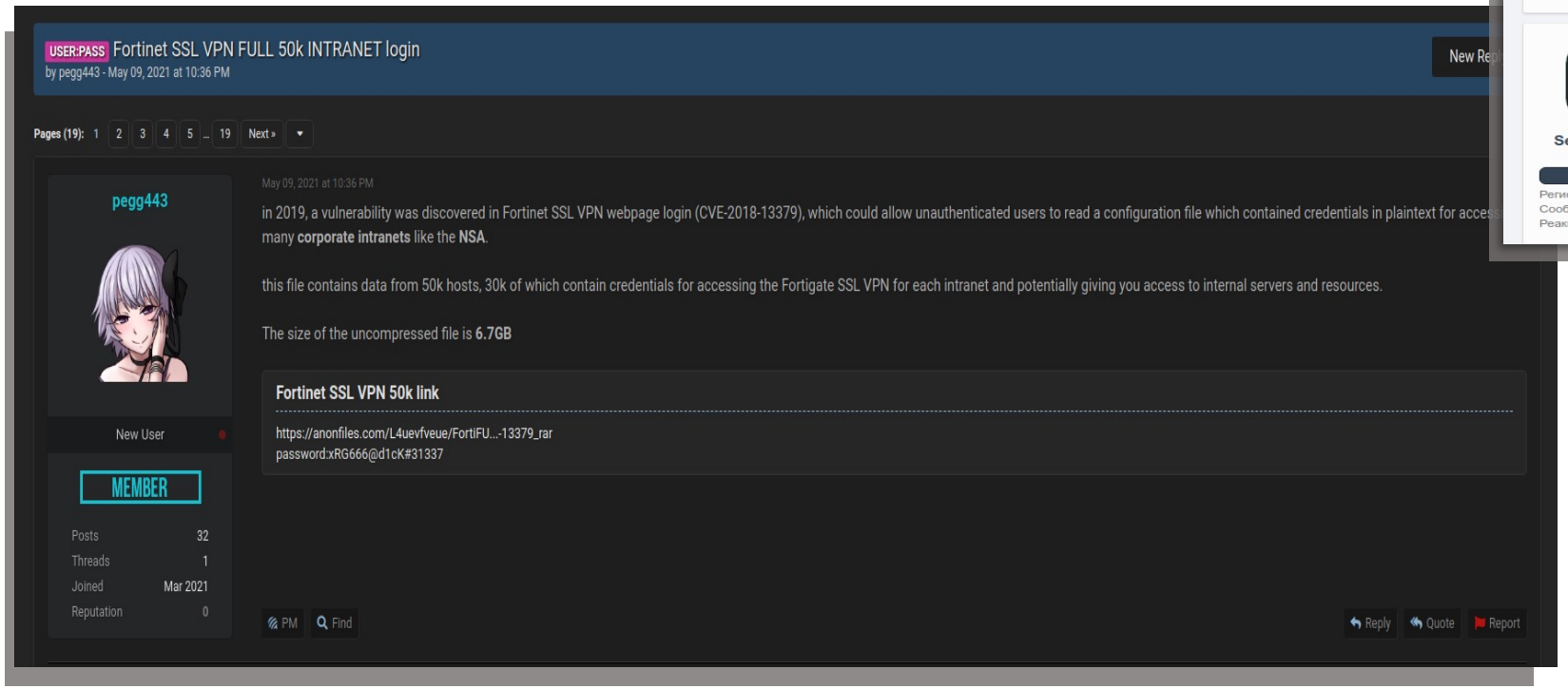


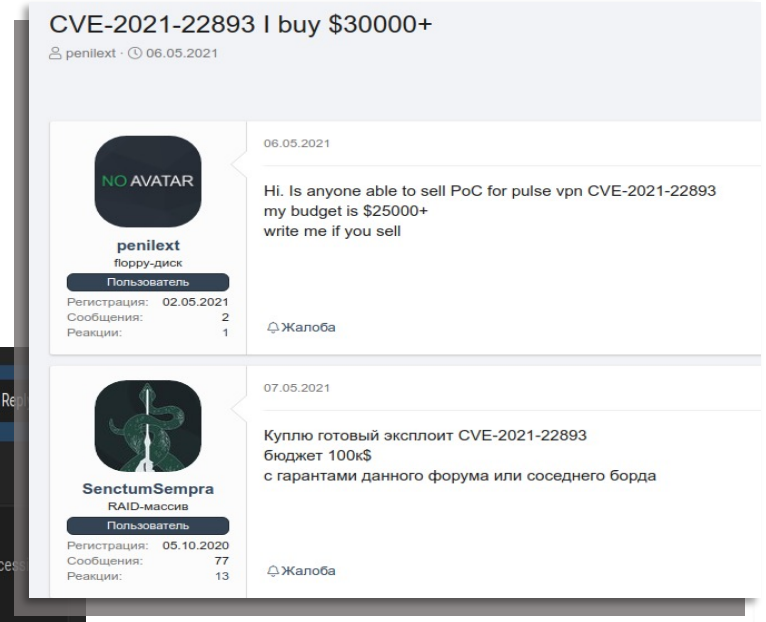


#WEINNOVATE

Target Site: qty3gmiq3zhs7whorla4ynvmndppmn5rgcuvsltgz7xl6xnxdxtp6zqd.onion

Cybercrime prevention





#WEINNOVATE

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

Conti Leak → see https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak
Attack Tactics, Techniques, Procedures → see Mitre Att@ck project (https://attack.mitre.org/) - https://attack.mitre.org/tactics/TA0001/

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

CYBER ACT FORUM 2021

WÜRTHPHOENIX

Thank you
Grazie Danke