





# Practical Dark Web Hunting using Automated Scripts

Apurv Singh Gautam  
@ASG\_Sc0rpi0n

# \$whoami

- Apurv Singh Gautam (@ASG\_Sc0rpi0n)
- Threat Researcher @ Cyble
- Cybersecurity @ Georgia Tech (Go Jackets) 
- Presented at conferences



- Hobbies
  - Hiking 
  - Lockpicking 
  - Gaming/Streaming



- Social
  - Twitter - @ASG\_Sc0rpi0n
  - Website - apurvsinghgautam.me

# Few Points

- ◎ This is an introduction to automating dark web hunting
- ◎ There are many more tools/methodologies than just the ones I will be covering
- ◎ We will discuss few advanced automation points but there will be no codes shown on that

# Agenda

- ◎ Why focusing on the Dark Web?
- ◎ Methods to hunt on the Dark Web
- ◎ Lab Time
- ◎ Scraping Defenses Discussion
- ◎ OpSec? What's that?
- ◎ Conclusion



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with concentric rings, and the lines are thin and grey. The diagram is partially cut off by the left edge of the frame.

# 1. Why focusing on the Dark Web

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a web of interconnected nodes and lines, with nodes represented by circles of varying sizes. The diagram is also partially cut off by the right edge of the frame.

# Why So Serious (Eh! Important)?

- ◎ Hacker forums, darknet markets, dump shops, etc.
- ◎ Criminals can learn, monetize, trade, and communicate
- ◎ Identification of compromised assets
- ◎ Can potentially identify attacks in earlier stages
- ◎ Direct impacts – PII (Personal Info), financial, EHRs (healthcare records), trade secrets
- ◎ Indirect impacts – reputation, revenue loss, legal penalties




# Why should you care?



**AW\_cards**  
Premium  
Premium

registration: 05/21/2021  
Posts: 57  
Reactions: 61  
Deposit: 0.27 \$

08/02/2021



# ALLWORLD CARDS

We publish 1,000,000 bank cards to the public .  
Valid is about 20% . All material from 2018-2019.  
Fields: CC\_Number Exp CVV Name Country State City Address Zip Email\_Phone

Promotion of unprecedented generosity from the store [AllWorld.Cards](#)

Checking the validity of random 98 cards Password from the archive - tor domain

Checked: 98 of 98  
Valid: 26 (27%)  
Total cost: 12.90\$

# Why should you care?

**SELLING** Access to second largest government owned Oil Company [REDACTED]

**Selling Access to Domain Network (Via Webshell)**

The Company is second largest government owned Oil [REDACTED]

Contact Only By DM Or My Telegram ID : [REDACTED]

Middleman Payment Acceptable

The Access Will Sell To One Person

www[REDACTED].com

Views: 36792

Website Website: www[REDACTED].com

Employees Employees: 7,100

Revenue Revenue: \$3 Billion Stock Symbol Stock Symbol: OIL

[https://www.zoominfo.com/\[REDACTED\]](https://www.zoominfo.com/[REDACTED])

If [REDACTED] won't continue negotiation process - we will begin publishing internal documentation, contracts, clients information and corporate messaging chats



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or central structure. The lines are thin and grey, connecting the nodes in a non-linear fashion.

2.

## Methods to hunt on the Dark Web

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, showing a web of interconnected nodes and lines. The nodes are small circles, some with concentric circles, connected by thin grey lines.

# Readily Available Tools

- ◎ Search Engine tools
- ◎ Onion Link Collection tools
- ◎ Onion Link Scan tools
- ◎ Onion Link Scraping tools

All tools available at:

<https://github.com/apurvsinghgautam/dark-web-osint-tools>

# Search Engine Tools

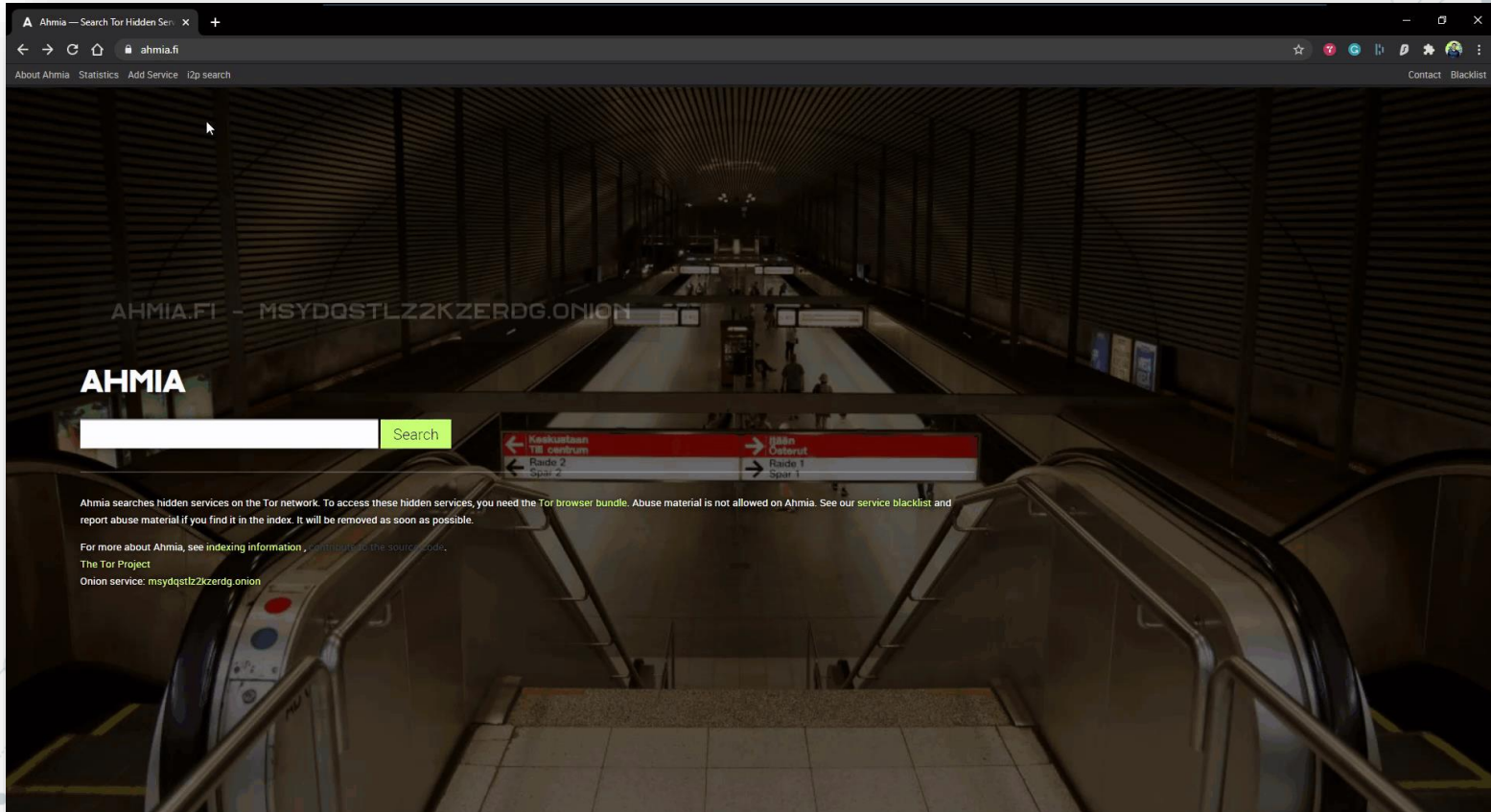
- ◎ Katana
- ◎ Onionsearch
- ◎ Ahmia Search Engine



**AHMIA**  
*Tor Anonymity Network Search Engine*

 **onion  
| Search**

# Ahmia



Ahmia — Search Tor Hidden Services

ahmia.fi

About Ahmia Statistics Add Service I2p search Contact Blacklist

AHMIA.FI — MSYDQSTLZ2KZERDG.ONION

**AHMIA**

Search

Ahmia searches hidden services on the Tor network. To access these hidden services, you need the [Tor browser bundle](#). Abuse material is not allowed on Ahmia. See our [service blacklist](#) and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see [indexing information](#), [contribute to the source code](#), [The Tor Project](#)

Onion service: [msydaqstlz2kzerdg.onion](https://msydaqstlz2kzerdg.onion)

# Onion Link Collection Tools

- © Hunchly
- © Tor66



# Hunchly

AutoSave On HiddenServices - Excel Search Gautam, Apurv Singh GA Share Comments

File Home Insert Page Layout Formulas Data Review View Help

Clipboard Font Alignment Number Styles Cells Editing Analysis Sensitivity

Calibri 11 A A' B I U Font Merge & Center General Conditional Formatting Format as Table Normal Bad Good Neutral Calculation Check Cell Explanatory... Input Insert Delete Format AutoSum Fill Sort & Filter Find & Select Analyze Data Sensitivity

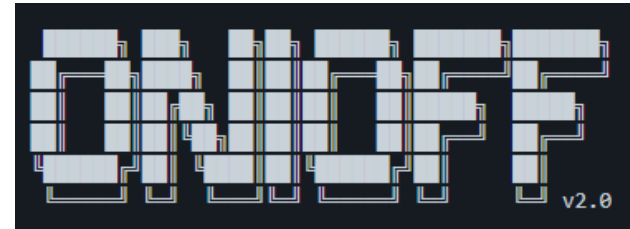
A1 Last Contacted

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Last Contacted	Hidden Service	Language	HTTP Stati	Last Up	Title									
2	2021-01-09 23:59:18	epynixtboxn4odv34z4eqnlampuwfz6uwmsamcqdi N/A	503	2020-02-17 19:53:39											
3	2021-01-09 10:06:19	9de135hfdvb961eefl.onion	N/A	503	Never										
4	2021-01-09 09:34:59	pegnetighusrp7nanuvncn5nt2vt65hhs6uaumdmt225 N/A	503	2020-10-15 21:11:06											
5	2021-01-09 23:28:42	deepdotweb35wvmeydd5.onion	N/A	503	Never										
6	2021-01-09 15:39:27	chanyucosmacristas.onion	N/A	503	Never										
7	2021-01-09 20:44:14	teamkden.crackedacctcon.onion	N/A	503	Never										
8	2021-01-09 05:12:42	hacker5quf443wtg4n7hi6m34xpcysknjvhhb6pcbga N/A	503	2020-12-26 12:46:54											
9	2021-01-09 17:39:24	youdonefuckedupnow.onion	N/A	503	Never										
10	2021-01-09 21:38:13	amazingd6g5zge7y.onionwikitorcjoweruxu.onion	N/A	503	Never										
11	2021-01-09 21:30:01	paoyu7gub72lykuk.onion	N/A	503	2021-01-08 22:55:56										
12	2021-01-09 10:35:00	wfflw5frtp5it4k.onion	N/A	503	2021-01-06 13:58:27										
13	2021-01-09 19:07:32	wbhkfwps2n33wde6l6w3ki4njikfie5ricqgfcjsh6rmlxc N/A	503	2020-04-01 23:19:20											
14	2021-01-09 10:39:36	prismsigadonepointone.onion	N/A	503	Never										
15	2021-01-09 17:09:42	6of3x4uhed5xqb4.onion	N/A	503	Never										
16	2021-01-09 04:06:37	adduser.3wz57p5b5mc7ubsjnzp4oxvqupeoywzwdxf N/A	503	Never											
17	2021-01-09 11:02:59	shadow57kjdjtx.onion	en	502	2019-07-11 00:21:24	502 - No server or forwarder data received (Privoxy@localhost)									
18	2021-01-09 15:06:34	rama.mayonaise.cabbage.tomatoes.onion	N/A	503	Never										
19	2021-01-09 09:31:14	3ubv4ppfed4o5kavu5uadp2r5jmm2j2x4j/bwtkwkbzh N/A	503	2019-04-23 12:20:21											
20	2021-01-09 11:55:41	xnwgk3hp7yne6kmlqpsizsx76oyjsnjlrvizyadjtr54zyt2 N/A	503	2020-04-04 13:21:57											
21	2021-01-09 21:21:17	qodvl3evhcmffavuzjasokl6stmqniybau2iskn4y2k7pkv N/A	503	2019-08-01 14:11:44											
22	2021-01-09 22:50:04	raymoll3svsudwh7vxuuajagocofwps25nq67zylibaew N/A	503	2020-10-16 20:02:14											
23	2021-01-09 12:01:03	bk4vfkf2fazxhs3pvg4t8gqx4puaej7hcsalkufulprkr2 N/A	503	2020-10-28 05:34:21											
24	2021-01-09 15:31:32	bv4saxizrmqmtqz25b5dxslle2brn46kx7gvnnhe7qgs2 N/A	503	2019-06-05 23:23:25											
25	2021-01-09 09:22:01	zmlg6gtdentfcvazvmawks7kzgdctlep72u44ktgjdj5p N/A	503	2020-09-22 10:55:01											
26	2021-01-09 20:29:09	sgeva4jy3sskldpd2ksyvnzvegi3khy3x75qhyzv4ogs5zn N/A	503	2019-04-22 02:43:56											
27	2021-01-09 13:56:17	aqjsj4lgyeleq6kxb54l2bbwxlr7zsoe2xnmawt43msq N/A	503	2019-09-12 08:30:09											
28	2021-01-09 20:03:11	jafojztdzgj07qcwq7wdip6elt3vedt3iy3zuds6xhipd N/A	503	2020-03-23 19:41:20											
29	2021-01-09 16:32:35	27ZdJ54621eannrcidfrance.onion	N/A	503	Never										
30	2021-01-09 16:14:38	smndqengabhaisw5t6j3g3wbvfhds4vt4nvpvgj46nl N/A	503	Never											
31	2021-01-09 16:04:40	Rjkgbtindukcunbtinrcvtocyt4dhkvct7oncdzcnk64dv N/A	503	Never											
32	2021-01-09 16:22:51	yjvt6hhwvaf44bzpqbg4rlluas6u375mgkmf3maa6tyjf N/A	503	2019-04-23 00:49:07											
33	2021-01-09 21:45:29	asfjasifadisiffoafcps.onion	N/A	503	Never										
34	2021-01-09 09:54:56	vy4ch3gie3sr6526t3u2ptbt5hw7ynklrlnfdm6oq43ar37 N/A	503	2020-11-19 02:37:36											
35	2021-01-09 20:55:17	ukranian-services.onion	N/A	503	Never										
36	2021-01-09 19:28:53	4nst65mv6z3abofj5r5wtit66ylxyrrtsquziuberzhkwkr N/A	503	2019-06-04 10:35:12											
37	2021-01-09 16:01:07	qxabu76bzgu5f6jw7mx56lwmk5znxnt5e4v2bfylwu N/A	503	2019-04-22 20:29:29											
38	2021-01-09 22:07:08	zphbuaiglb5bbhy4bpk56gbxzyhabr6iobvcxjircxy4tvt N/A	503	Never											

New Today Down Up

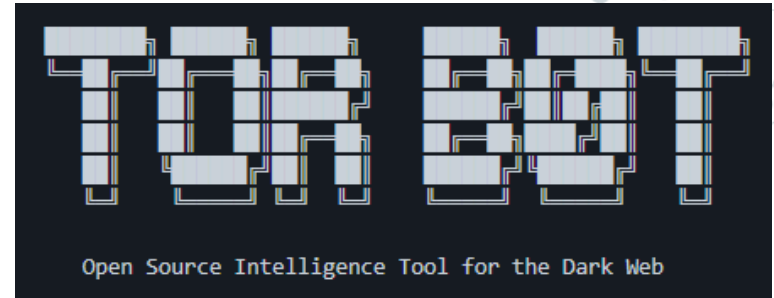
# Onion Link Scan Tools

- ◎ OnionScan
- ◎ Onioff
- ◎ Onion-nmap



# Onion Link Scraping Tools

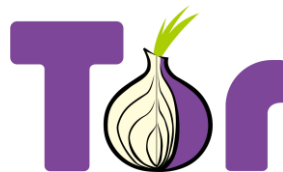
- ◎ TorBot
- ◎ TorCrawl
- ◎ OnionIngestor



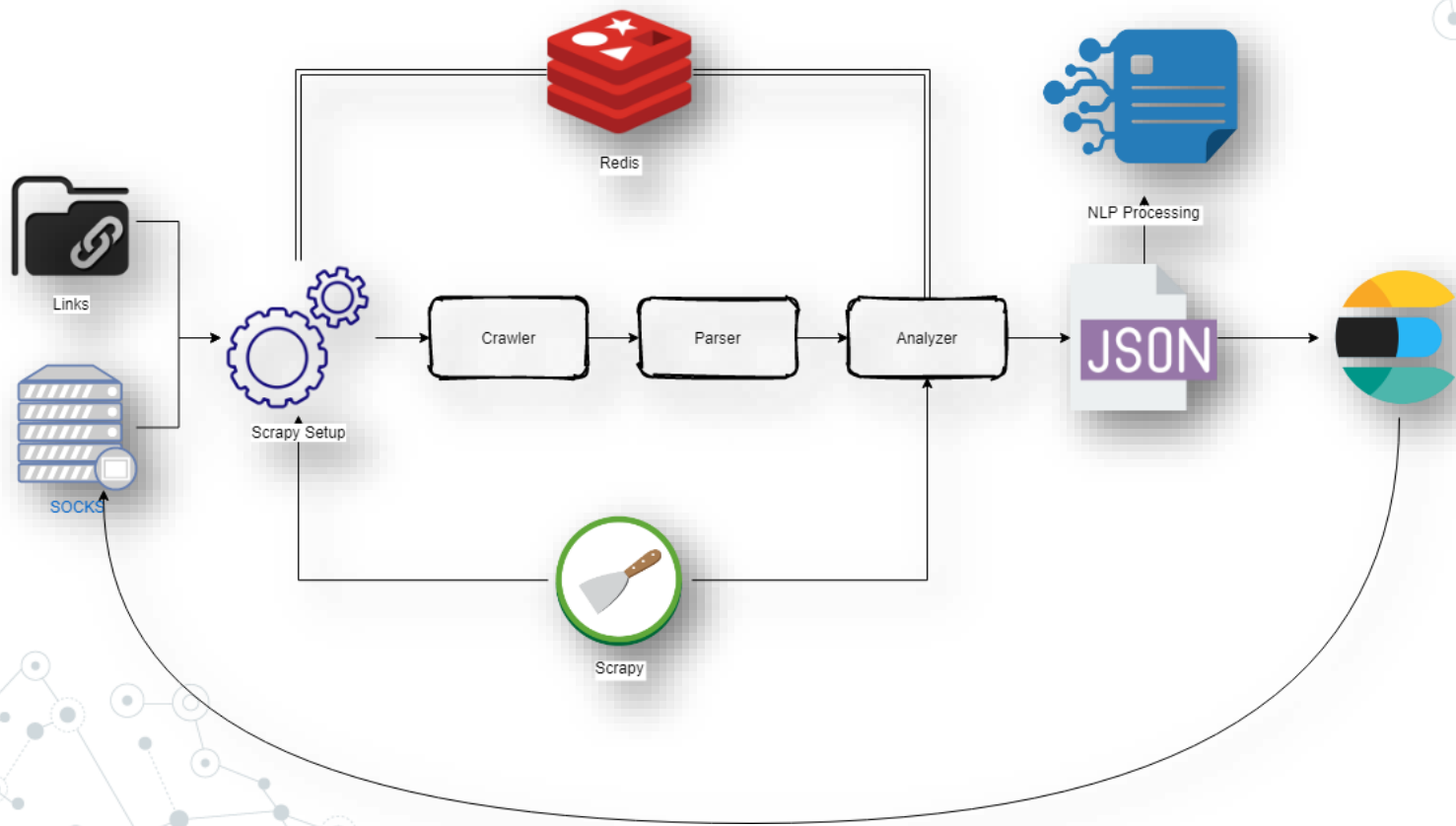


# Create your own hunting tools

- ◎ Scrapy
- ◎ Tor
- ◎ Privoxy
- ◎ Elastic
- ◎ and many more...



# Automated Hunting Architecture



# How Scrapy Works?

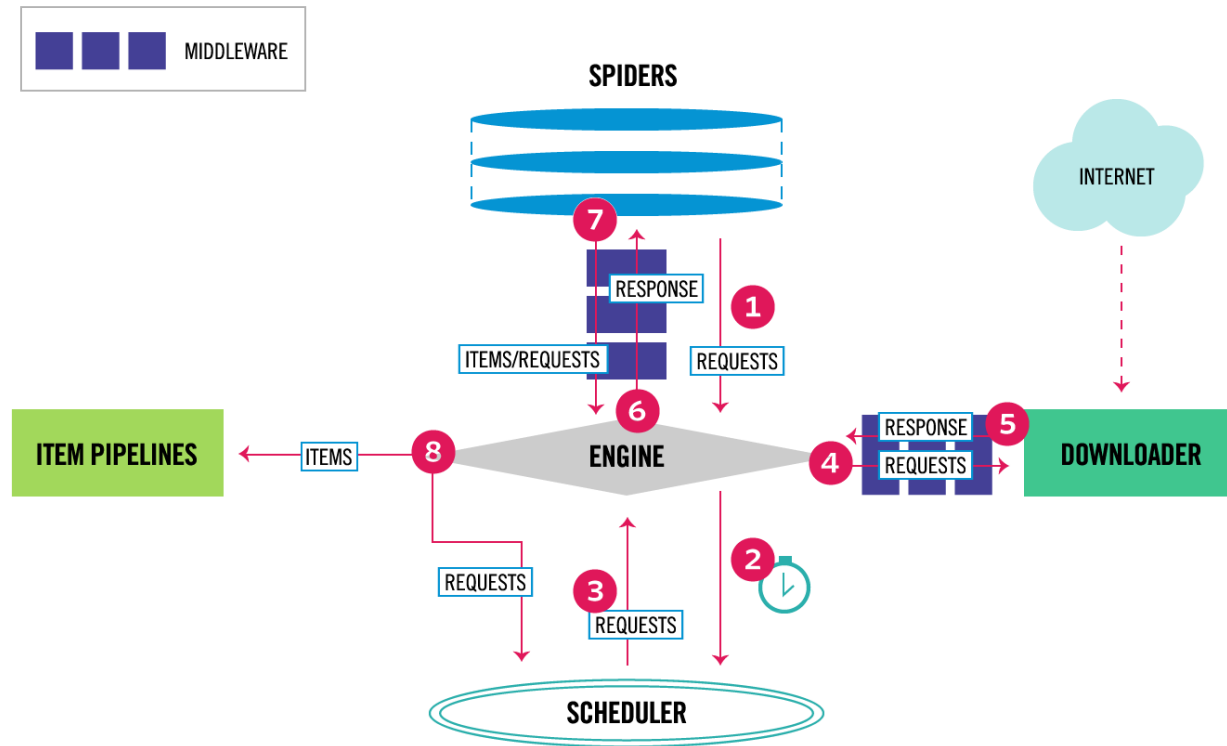


Image Source: Scrapy Docs



# 3. Lab Time



# Setting up a Lab

- ◎ Lab/VM
- ◎ Physical or Cloud
- ◎ Isolate the network
- ◎ Install relevant tools
  - Go
  - Scrappy
  - Privoxy
  - Tor
  - ELK
  - Go libraries
  - Python libraries



Image Source: Hayden James

# NZDarknet Forum








## NZ Darknet Market Forums

Darknet Market education and discussion

Index	User list	Rules	Search	Register	Login	
-------	-----------	-------	--------	----------	-------	--

You are not logged in.

» Topics: [Active](#) | [Unanswered](#)

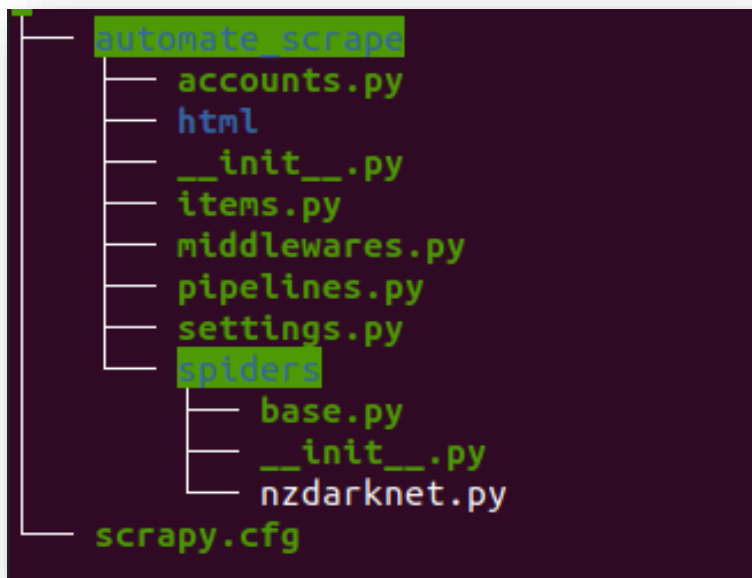
New Zealand darknet markets	Topics	Posts	Last post
 <b>General discussion</b> General darknet market use, bitcoin, TOR, VPNs, PGP.	466	2,645	2020-12-26 10:50 by Really
 <b>Product sourcing</b> Requests for products, demand enquiries	344	1,408	Today 00:30 by Pogo_The_Monkey
 <b>Product reviews</b> Detailed reviews of products and vendors	96	297	2020-12-12 16:10 by Metalmanne
 <b>Vendor updates</b> Vendor announcements, news and updates	92	226	2020-12-20 02:20 by goblins_shadow
Tor Market	Topics	Posts	Last post
 <b>General</b> Tor Market specific general discussion	87	451	2020-12-24 22:50 by NZDMFmod
 <b>Buyer help</b> Help with using buyer features of Tor Market	54	239	2020-12-03 00:40 by TormarketSupport
 <b>Vendor help</b> Help with using vendor features of Tor Market	34	95	Yesterday 15:20 by Xobia

Newest registered user: [Pogo\\_The\\_Monkey](#)

Total number of registered users: **2,982**  
Total number of topics: **1,237**  
Total number of posts: **5,705**

Jump to

# Tree Structure



# nzdarknet.py

```
BASE_URL = 'http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/'

class NZDarknetSpider(WebSpider):
    settings = get_project_settings()
    name = 'nzdarknet'
    forum_items = AutomateScrapeItem()
    default_start_url = None
    allowed_domains = ['nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion']
    start_urls = [
        'http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/index.php'
    ]

    # Rule to scrape all links
    # rules = (
    #     Rule(LinkExtractor(allow=r'page\/*.*', deny=r''), callback='parse_posts', follow=True),
    # )

    def start_requests(self):
        logging.info('Making first request')
        ##Logic

    def parse_forum(self, response):
        logging.info('In Parse Posts')
        ##Logic

    def save_page(self, response):
        logging.info('In Save Page')
        ## Logic
```



# middlewares.py

```
import logging
from scrapy import signals
from .accounts import accounts
from scrapy.utils.project import get_project_settings

class ProxyMiddleware(object):

    def process_request(self, request, spider):
        # request.current_user = random.choice(accounts)
        # proxy = request.current_user['proxy'][0]

        proxy = {
            'ip': '127.0.0.1',
            'port': '9000'
        }
        request.meta['proxy'] = 'http://{}:{ {}'.format(proxy['ip'], proxy['port'])
        logging.info("Setting proxy {}".format(request.meta['proxy']))
```

# items.py

```
import scrapy

class AutomateScrapeItem(scrapy.Item):
    timestamp = scrapy.Field()
    forum_category = scrapy.Field()
    post_title = scrapy.Field()
    post_date = scrapy.Field()
    post_author = scrapy.Field()
    post_author_url = scrapy.Field()
    post_body = scrapy.Field()
    post_replies = scrapy.Field()
```

# pipelines.py

```
class JSONPipeline(object):

    def process_item(self, item, spider):
        logging.info('In JSON Pipeline')
        logging.info(item)
        if 'timestamp' in item:
            data = {
                'timestamp': item['timestamp'],
                'forum_category': item['forum_category'],
                'post_title': item['post_title'],
                'post_date': item['post_date'],
                'post_author': item['post_author'],
                'post_author_url': item['post_author_url'],
                'post_body': item['post_body'],
                'post_replies': item['post_replies']
            }
            json_list.append(data)

        dumped = json.dumps(json_list, indent=4, ensure_ascii=False)
        file = open('data_from_pipeline.json', 'a+')
        file.write(dumped + '\n')
        file.close()
        return item
```

# settings.py

```
BOT_NAME = 'automate_scrape'

SPIDER_MODULES = ['automate_scrape.spiders']
NEWSPIDER_MODULE = 'automate_scrape.spiders'

# Crawl responsibly by identifying yourself (and your website) on the user-agent
USER_AGENT = 'User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0'

# Obey robots.txt rules
ROBOTSTXT_OBEY = False

# Configure maximum concurrent requests performed by Scrapy (default: 16)
CONCURRENT_REQUESTS = 32

# Configure a delay for requests for the same website (default: 0)
# See https://docs.scrapy.org/en/latest/topics/settings.html#download-delay
# See also autothrottle settings and docs
DOWNLOAD_DELAY = 5
# The download delay setting will honor only one of:
#CONCURRENT_REQUESTS_PER_DOMAIN = 16
#CONCURRENT_REQUESTS_PER_IP = 16

# Override the default request headers:
DEFAULT_REQUEST_HEADERS = {
    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8',
    'Accept-Language': 'en-US,en;q=0.5',
    'Connection': 'keep-alive'
}

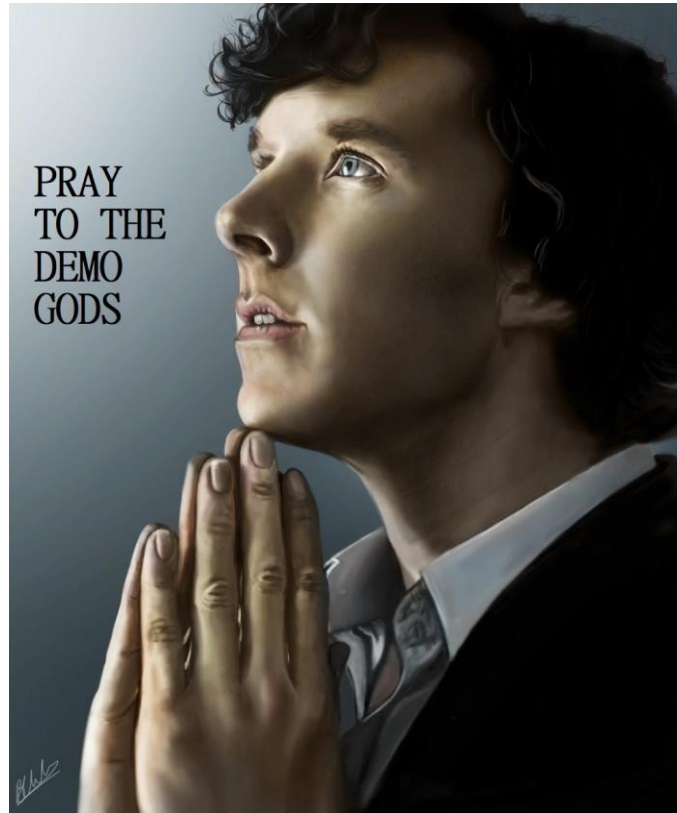
# Enable or disable downloader middlewares
# See https://docs.scrapy.org/en/latest/topics/downloader-middleware.html
DOWNLOADER_MIDDLEWARES = {
    'automate_scrape.middlewares.ProxyMiddleware': 50
}

# Configure item pipelines
# See https://docs.scrapy.org/en/latest/topics/item-pipeline.html
ITEM_PIPELINES = {
    'automate_scrape.pipelines.JSONPipeline': 50
}
```

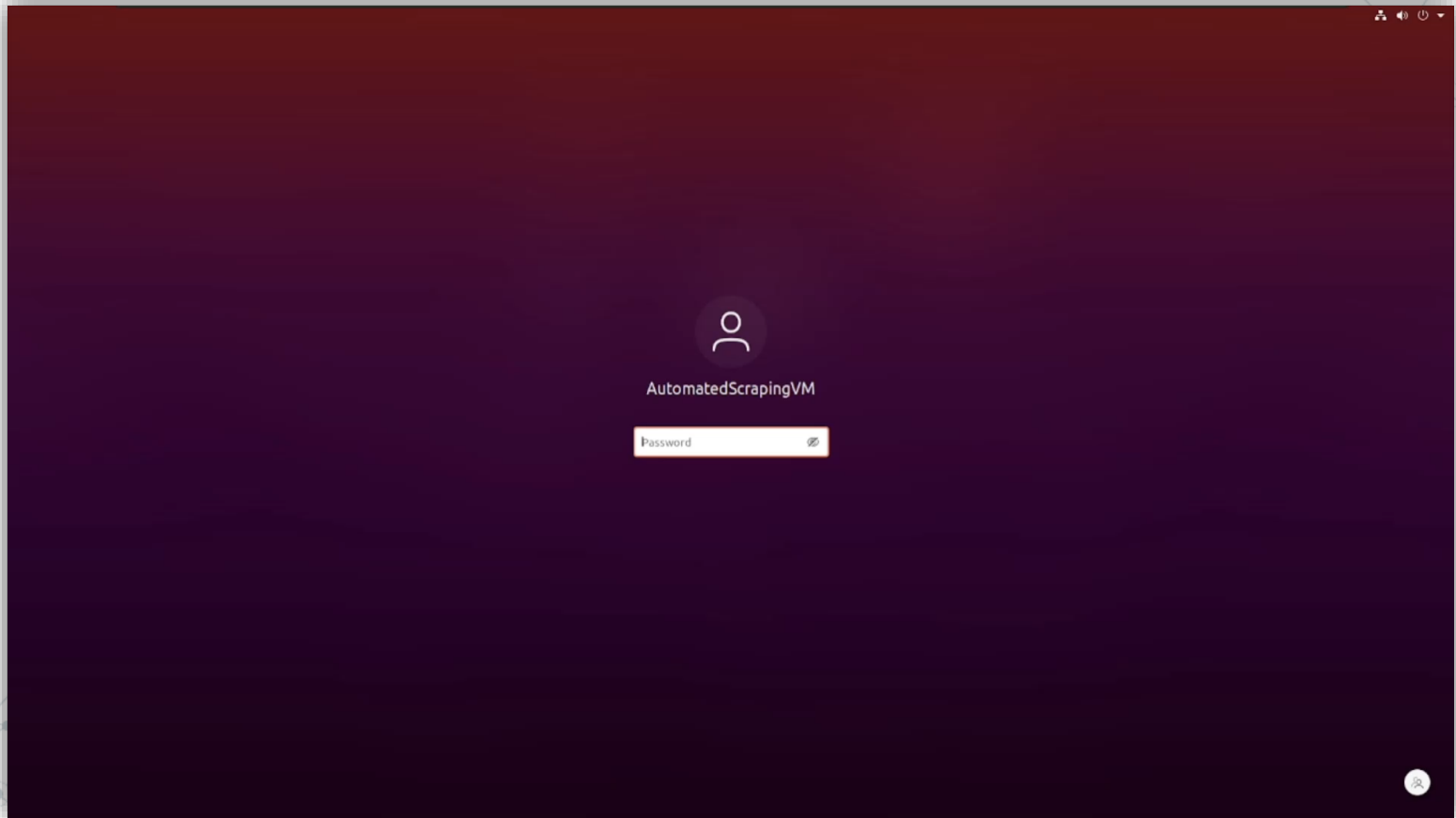
# Sample JSON Data

```
{
  "timestamp": "2022-01-16T18:35:21",
  "forum_category": "General discussion",
  "post_title": "Links/URLs for markets and other DNM content",
  "post_date": "2019-05-05 15:00",
  "post_author": "TormarketSupport",
  "post_author_url": "http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/profile.php?id=2",
  "post_body": "\n\t\t\t\t\t DarknetLive news, market links, dnm bible pdf. Dark.fail news, market links Recon Software https://tails.
  "post_replies": [
    {
      "reply": 1,
      "post_date": "2020-05-03 01:10",
      "post_author": "TormarketSupport",
      "post_author_url": "http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/profile.php?id=2",
      "post_body": "\n\t\t\t\t\t ----BEGIN PGP SIGNED MESSAGE-----\nHash: SHA512\n\nNew primary Tormarket URL\n\nhttp://rrlm2f22lpg
    },
    {
      "reply": 2,
      "post_date": "2021-01-11 14:20",
      "post_author": "TormarketSupport",
      "post_author_url": "http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/profile.php?id=2",
      "post_body": "\n\t\t\t\t\t ----BEGIN PGP SIGNED MESSAGE----- Hash: SHA512 The old retired Tormarket onion v2 is http://tt2mop
    },
    {
      "reply": 3,
      "post_date": "2021-01-11 19:00",
      "post_author": "TormarketSupport",
      "post_author_url": "http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/profile.php?id=2",
      "post_body": "\n\t\t\t\t\t Clickable links for Tormarket Tormarket old version tt2mopgckifmberr.onion Tormarket p5ay4zakxz4r
    },
    {
      "reply": 4,
      "post_date": "2021-06-24 10:10",
      "post_author": "ChurBroNZ",
      "post_author_url": "http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/profile.php?id=2903",
      "post_body": "\n\t\t\t\t\t Appears the script kids are at it again! Using backup link. \n\t\t\t\t\t"
    },
    {
      "reply": 5,
      "post_date": "2021-06-24 14:40",
      "post_author": "TormarketSupport",
      "post_author_url": "http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/profile.php?id=2",
      "post_body": "\n\t\t\t\t\t p5ay4zakxz4rn4rmvx6c3vj3fj2jLzbsgg5a2xrgrjz92tsw2uogmuyd<0xa0> will always be more reliable because
    }
  ]
}
```

# Demo



# Demo Video



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some solid and some hollow, connected by thin lines. The overall structure is dense and organic, resembling a molecular or biological network.

4.

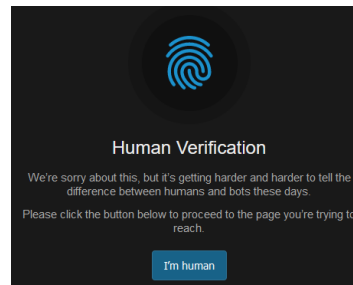
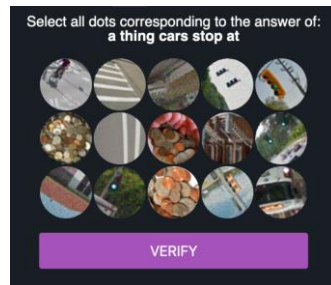
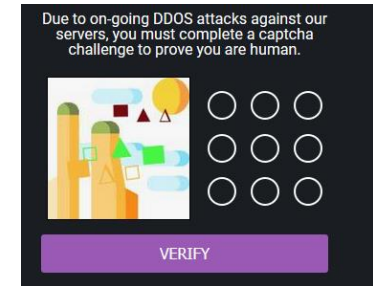
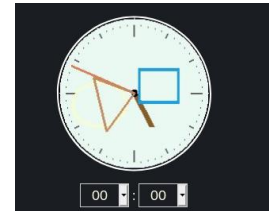
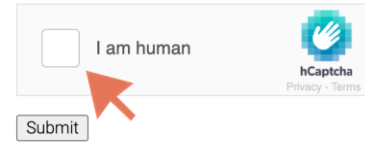
# Scraping Defenses Discussion

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes highlighted by concentric circles. The diagram is positioned in the bottom-right corner of the slide.



# What defenses do sites put?

- ◎ DDoS Protection
- ◎ Captcha System
- ◎ JavaScript Enabled Sites
- ◎ IP blocking
- ◎ Account blocking
- ◎ Cookie Change



# Circumventing Scraping Defenses

- ◎ Setting Delays
- ◎ Captcha Bypass Services
- ◎ Using Selenium
- ◎ Rotating IPs (SOCKS 4/5)
- ◎ Rotating Accounts
- ◎ Utilizing different Cookies

# Circumventing Scraping Defenses

```
from selenium import webdriver

url = ''
path = ''

driver = webdriver.Firefox()
driver.get(url)
el = driver.find_element_by_tag_name('body')
el.screenshot(path)
driver.quit
```

```
class CookieMiddleware(object):
    I
    def process_request(self, request, spider):
        if request.cookies == {}:
            logging.info("Setting cookie for User {}".format(request.current_user['user']))
            request.cookies = self.get_cookies(request)
        return None

    def get_cookies(self, request):
        #logic for getting cookies from file
        return cook
```

```
class CheckCookieMiddleware(object):

    def __init__(self):
        self.bot = telebot.TeleBot(API_KEY, parse_mode=None)

    def process_response(self, request, response, spider):
        if '503' in response.text:
            #telegram reminder msg
            self.bot.send_message(UID, 'URGENT: Change Cookie'))
            # Ctrl+C signal
            os.kill(os.getpid(), signal.SIGINT)
        return response
```

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some solid and some hollow, connected by thin lines. The overall structure is a dense, branching network.

5.

OpSec? What's  
that?

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some solid and some hollow, connected by thin lines. The overall structure is a dense, branching network.

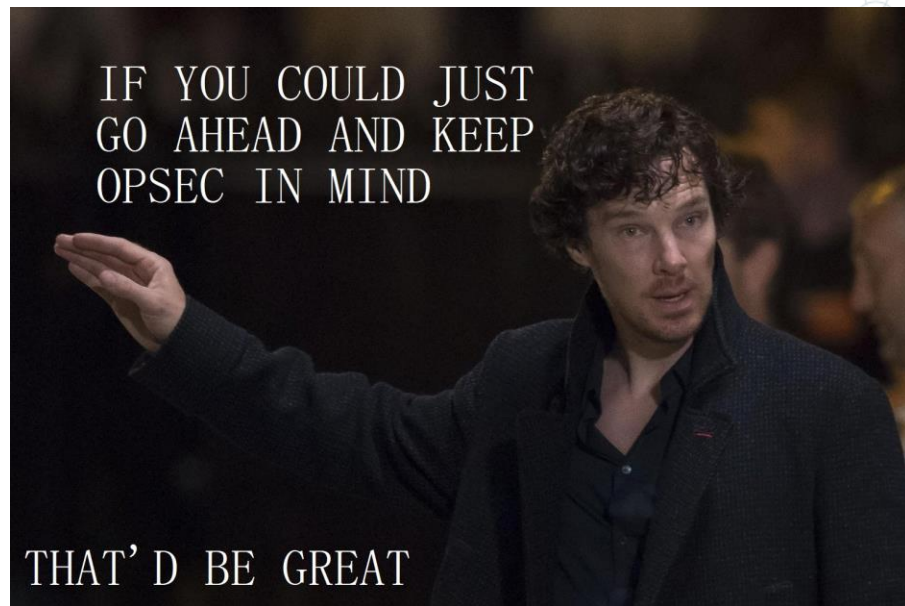
# What is OpSec?

- ◎ Actions taken to ensure that information leakage doesn't compromise you or your operations
- ◎ Derived from US military – Operational Security
- ◎ PII – Personally Identifiable Information
- ◎ Not just a process – a mindset
- ◎ OpSec is Hard



# Maintaining OpSec in your lifestyle

- ◎ Use VM/Lab or an isolated system
- ◎ Use Tor over SOCKS or VPN
- ◎ Change Time zones
- ◎ Maintain different persona
- ◎ Use password manager
- ◎ Clean/Wipe data from VM
- ◎ Say NO to personal info



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or multi-layered structure. The lines are thin and gray, connecting the nodes in a non-linear fashion.

# 6. Conclusion

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or multi-layered structure. The lines are thin and gray, connecting the nodes in a non-linear fashion.

# What we discussed so far?

- ◎ Why Dark web hunting is important
- ◎ Tools needed to hunt data on the Dark Web
- ◎ OSINT Tools
- ◎ Methods to create your own hunting scripts
- ◎ Automating the data collection
- ◎ Scraping defenses circumvention



# I don't know how to conclude but..

- ◎ Keep OpSec in mind
- ◎ Look at more than one resource/site
- ◎ Takes a lot of resources and team effort
- ◎ Unique ways to create your automated architecture

# Resources

- ◎ Read White papers & blogs from different security organizations
- ◎ Follow people on LinkedIn and Twitter
- ◎ Follow hashtags - #darkweb, #threatintelligence
- ◎ Search Terms – darkweb, tor, deepweb, cybercrime forums
- ◎ OSINT Framework - <https://osintframework.com/>
- ◎ OSINT Combine Dark Web Searching - <https://www.osintcombine.com/post/dark-web-searching>

# Resources (Contd.)

- ◎ Jake Creps Blog - <https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/>
- ◎ SANS OSINT Summit – OSINT Tools for Diving deep into the Dark Web
- ◎ DEFCON Recon Village - Ambly the Smart Darknet Spider talk by Cytisus Eurydice (@levitannin)
- ◎ Darkweb Cyber Threat Intelligence Mining by Cambridge University Press



# Any questions?

For Virtual - Q/A in #btv-workshops-text

For In-Person – I will be around LINQ for Skytalks (Come say Hi!)

# Thanks!

You can contact me at:

Twitter: @ASG\_Sc0rpi0n

LinkedIn: /in/apurvsinghgautam

