

A decorative background graphic consisting of a network of nodes and edges. The nodes are represented by small circles, some of which are highlighted with a blue outline. The edges are thin, light gray lines connecting the nodes. The network is distributed across the top-left and bottom-right corners of the slide, framing the central text.

# Automating Threat Hunting on the Dark Web and other nitty-gritty things

# \$whoami

- ◎ Apurv Singh Gautam (@ASG\_Sc0rpi0n)
- ◎ Security Researcher, Threat Intel/Hunting
- ◎ Cybersecurity @ Georgia Tech
- ◎ Prior: Research Intern at ICSI, UC Berkeley
- ◎ Hobbies
  - ◎ Contributing to the security community (Cybrary)
  - ◎ Gaming/Streaming (Rainbow 6 Siege)
  - ◎ Hiking, Lockpicking
- ◎ Social
  - ◎ Twitter - @ASG\_Sc0rpi0n
  - ◎ Website – <https://apurvsinghgautam.me>

# Agenda

- ◎ Introduction to the Dark Web
- ◎ Why hunting on the Dark Web?
- ◎ Methods to hunt on the Dark Web
- ◎ Can Dark Web hunting be automated?
- ◎ 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. Introduction to the Dark Web

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

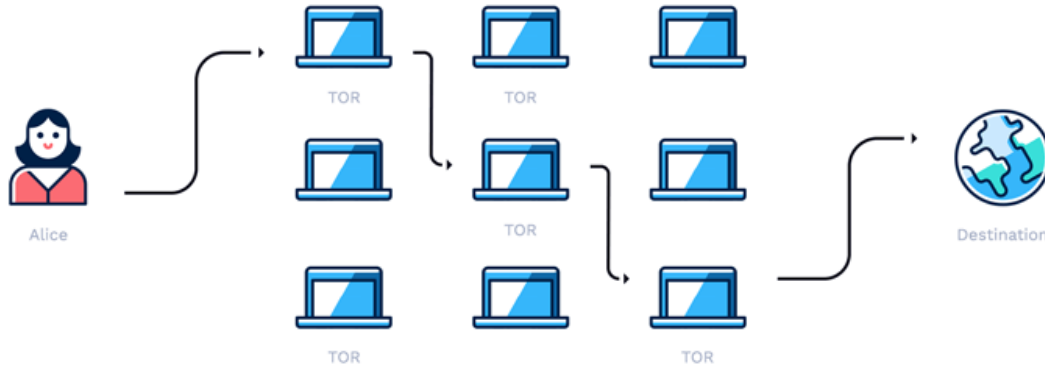
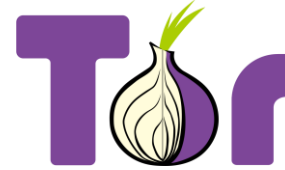
# Clear Web? Deep Web? Dark Web?



Image Source: UC San Diego Library

# Accessing the Dark Web

- ◎ Tor /I2P/ZeroNet
- ◎ .onion domains/.i2p domains
- ◎ Traffic through relays



# Relevant site types?

- ◎ General Markets
- ◎ PII & PHI
- ◎ Credit Cards
- ◎ Digital identities
- ◎ Information Trading
- ◎ Remote Access
- ◎ Personal Documents
- ◎ Electronic Wallets
- ◎ Insider Threats

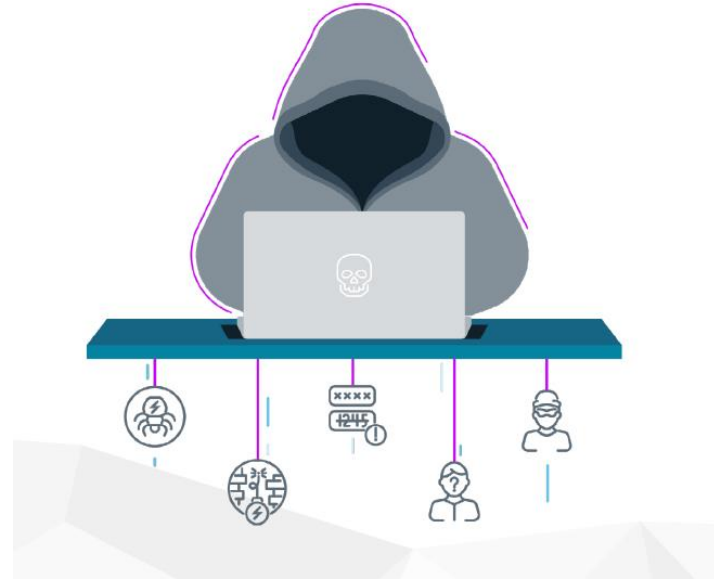


Image Source: Insights

# Sites Examples

## Whistleblowing

- [WikiLeaks](#) - DeepWeb mirror of the famous Wikileaks website.
- [Doxbin](#) - A pastebin for personally identifiable information.
- [SecureDrop](#) - The open-source whistleblower submission system managed
- [Active at Darknet Markets?](#) - Onion set up by the Police and the Judicial A arrested Darknet Market operators.
- [Cryptome](#) - Archive Government Leaks. Documents for publication that are prohibited by governments worldwide, in particular material on freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and secret governance -- open, secret and classified documents
- [SecureDrop](#) - An open-so from and communicate with

## H/P/A/W/I/C

Hack, Phreak, Anarchy (internet), Warez, Virus, Crack

- [HeLL Forum](#) - HeLL Reloaded is back!
- [RelateList](#) - New era of intelligence.
- [CODE: GREEN](#) - Ethical hacktivism for a better world. Join us and participate in modern world protests!
- [Hack Canada](#) - America is a joke and Canada is the punchline. Old-ish hacking site, hosts a few archives.
- [Hacker Place](#) - Site with several books and resources on software development, pentesting and hacking.
- [WE fight censorship](#) - a Reporters Without Borders project that aims to combat censorship and promote the flow of news and information.

## 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.
- [The Paypal World](#) Paypal accounts with good balances - buy some, and fix your financial situation for awhile.
- [Premium Cards](#) Oldest cc vendor, Top quality Us & Eu credit cards!
- [Financial Oasis](#) A slew of products from a darker side of finance.



# Product Examples

**USA FRESH CREATED BANK OF AMERICA BANK DROP + EMAIL ACCESS + PHONE ACCESS + DEBIT CARD + COOKIES**  
 -ALLOW 1-5 DAYS FOR DELIVERY UPON ORDERING YOU WILL RECEIVE

Sold by **MasterSplinter0** - 20 sold since March 22, 2020 **Vendor Level 1**

Product Class	Features	Origin Country
Digital	Unlimited	Ships to Payment
Quantity Left	Never	
Ends In		

Default - 4 days - USD + 0.00 / order

Purchase price: **USD 90.00**

Qty:  **Buy Now** **Buy Now** **Queue**

0.009610 BTC / 1.389318 XMR

**NordVPN.com - [LIFETIME NORDVPN PREMIUM ACCOUNT]**  
 Website: <https://nordvpn.com> Imagine VPN as a hack-proof, encrypted tunnel for online traffic to flow. Nobody can see thr...

Sold by **MissPinky** - 95 sold since December 11, 2019 **Vendor Level 4** **Trust level 4**

Unlimited items available for auto-dispatch

Product Class	Features
Digital	Unlimited
Quantity Left	Never
Ends In	

Private Message - 1 days - USD + 0.00 / order

Purchase price: **USD 9.99**

Qty:  **Buy Now** **Buy Now**

0.001067 BTC / 0.229919 LTC / 0.154214 XMR

Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.15780 B	<input type="text" value="1"/> X <b>Buy now</b>
Netherlands Passport	1500 EUR = 0.17533 B	<input type="text" value="1"/> X <b>Buy now</b>
Denmark Passport	1500 EUR = 0.17533 B	<input type="text" value="1"/> X <b>Buy now</b>

## Rent-A-Hacker

Experienced hacker offering his services (Illegal) Hacking and social engineering. I'm really good at hacking and I made a lot of money. I have worked for other people before.



## USA Bank login Cracker Bruter

banks: bruteforcecheck 2020...guys here is all bank bruter, its really easy to use all u need is a good combo list and proxies

Sold by **TheCashier** - 3 sold since April 28, 2020 **Vendor Level 1** **Trust level 2**

Unlimited items available for auto-dispatch

Product Class	Features
Digital	Unlimited
Quantity Left	Never
Ends In	

default - 1 day - USD + 0.00

Purchase price: **USD 3.00**

Qty:  **Buy Now** **Buy Now**

0.000319 BTC / 0.068368 LTC / 0.045537 XMR

**VISA Virtual Card**

Valid only for use in the United states

**VISA**

Visa® Virtual Account

Account Number: 4000 1234 5678 9010

Valid Thru: 12/23

DEBIT GIFT

5000 Virtual card: \$250  
15000 Virtual card: \$730  
7500 Virtual card: \$375  
20000 Virtual card: \$880  
10000 Virtual card: \$490  
25000 Virtual card: \$1050

**Virtual MasterCard (USD)**

Valid Worldwide, All the World

**PREPAID**

5362 0588 8888 8888

Cardholder: 0000

mastercard

Price

500 Giftcard: \$280  
1500 Giftcard: \$730  
750 Giftcard: \$390  
1750 Giftcard: \$850  
1000 Giftcard: \$500  
2000 Giftcard: \$950

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and red.

2.

## Why hunting on the Dark Web

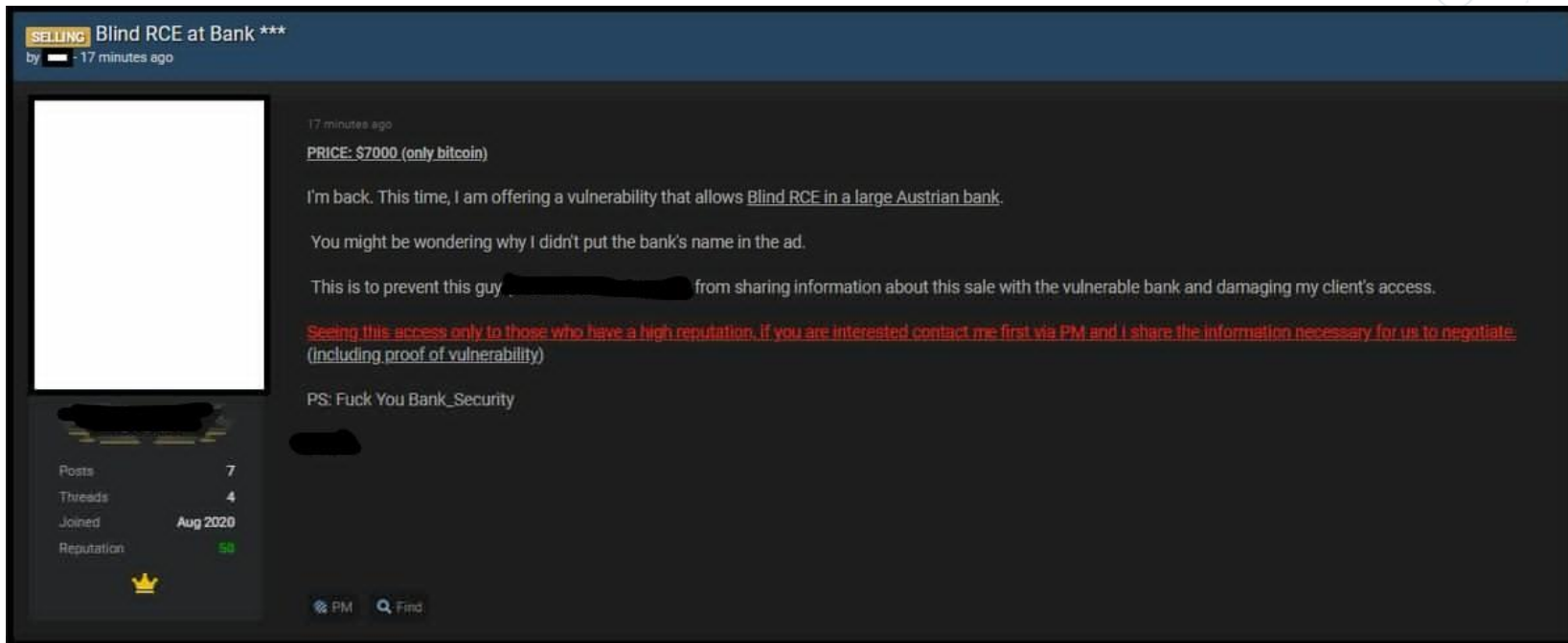
A decorative network diagram in the bottom-right corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and red.

# 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 you should care?



**SELLING** Blind RCE at Bank \*\*\*  
by [redacted] - 17 minutes ago

17 minutes ago  
**PRICE: \$7000 (only bitcoin)**

I'm back. This time, I am offering a vulnerability that allows Blind RCE in a large Austrian bank.

You might be wondering why I didn't put the bank's name in the ad.

This is to prevent this guy [redacted] from sharing information about this sale with the vulnerable bank and damaging my client's access.

Seeing this access only to those who have a high reputation. If you are interested contact me first via PM and I share the information necessary for us to negotiate. (including proof of vulnerability)

PS: Fuck You Bank\_Security  
[redacted]

**User Profile:**

- Posts: 7
- Threads: 4
- Joined: Aug 2020
- Reputation: 53

PM Find

# Why you should care?

## Untitled 53704


Anon, September 18, 2020 - 7:59 am UTC




Prime Health Care Services has serious "Cyber Security vulnerability's within their hospital's across America.

Specifically those in the RGV, and Mission Regional Medical Center are easy to deploy Rats, and compromise Cyber Security for a treasure trove of information / dox.

Also their physical security while not in the covid 19 pandemic is pretty lame if you know what I mean you can get away with just about anything as pimple the frog from Battle Toads does in the movie Patriots Day.

# Why you should care?

**USA Hospital RDP For Sale - Больница США RDP на продажу**  
September 4 in Auctions

  
  
Paid registration  
1  
68 posts  
Joined  
  
Activity  
вирусология / malware

Posted September 4 (edited)

Selling RDP of a US Hospital.

On the RDP has a lot of patient records and also active software client which shows full medical records of patients etc.

I have no use for this topic. You will receive login information of the RDP in one hand.

Willing to work through escrow/guarantor (buyer pays fees)

Start: \$ 500

Step: \$ 100

Blitz: \$ 5000

Auction is valid only for 24hours!

=====

Продам РДП больницы США.

На RDP есть много записей пациентов, а также активный программный клиент, который показывает полные медицинские карты пациентов и т. Д.

Мне эта тема не нужна. Вы получите данные для входа в RDP в одни руки.


Готовность работать через эскроу / поручителя (комиссию оплачивает покупатель)


Старт: \$ 500

Шаг: \$ 100

Блиц: \$ 5000

Аукцион действителен только 24 часа!



 Quote

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.

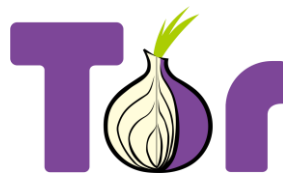
3.

# 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 complex web of interconnected nodes and lines.

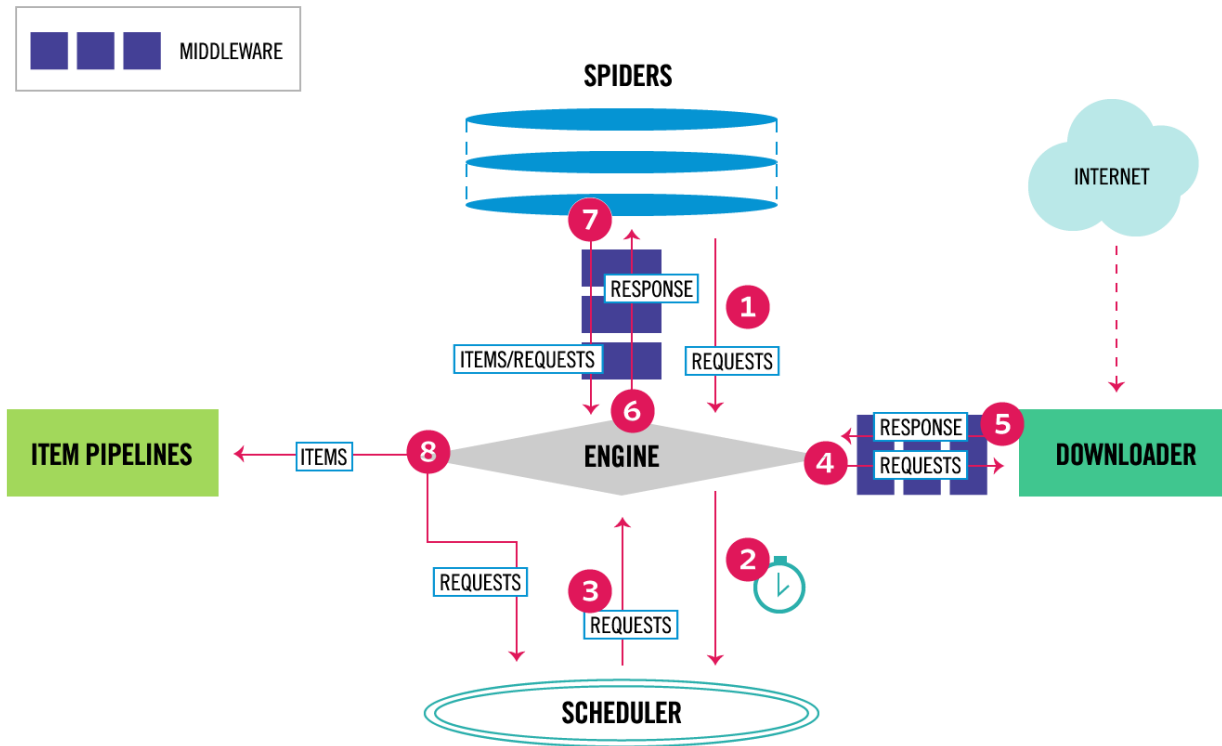
# Tools

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





# How Scrapy Works?



# HUMINT

- ◎ Human Intelligence
- ◎ Most dangerous and difficult form
- ◎ Most valuable source
- ◎ Infiltrating forums, markets, etc.
- ◎ Become one of them
- ◎ How threat actors think
- ◎ Can be very risky
- ◎ Time consuming

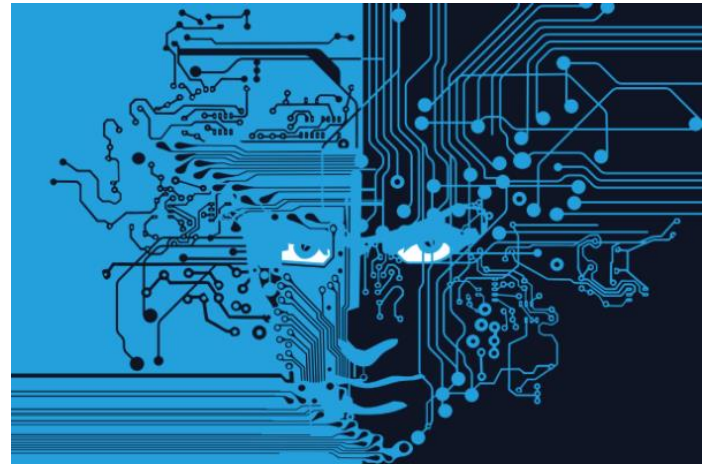


Image Source: Intsights

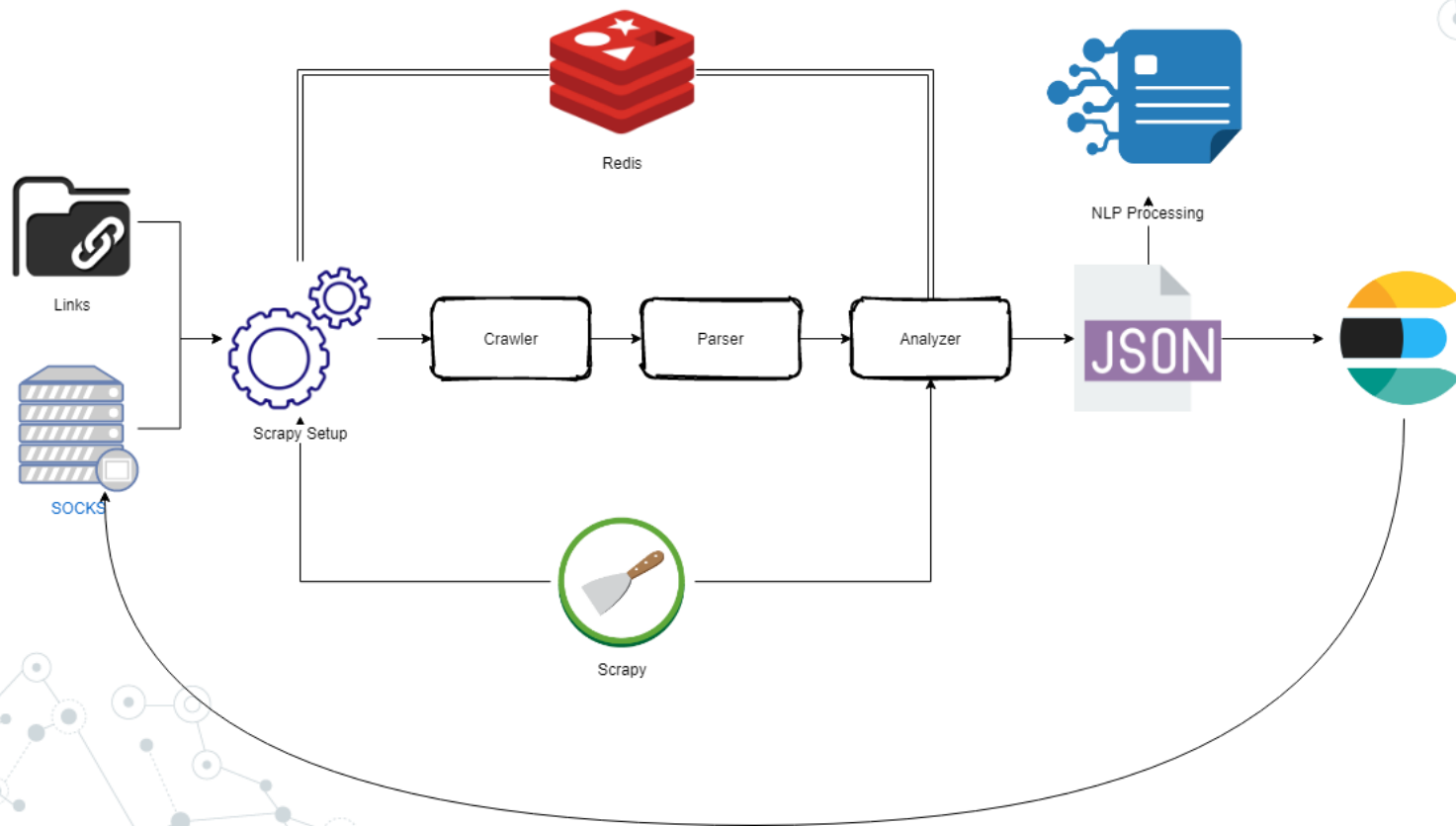
A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

4.

**Can Dark Web hunting  
be Automated?**

A decorative network diagram in the bottom-right corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

# Automated Hunting Architecture



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.

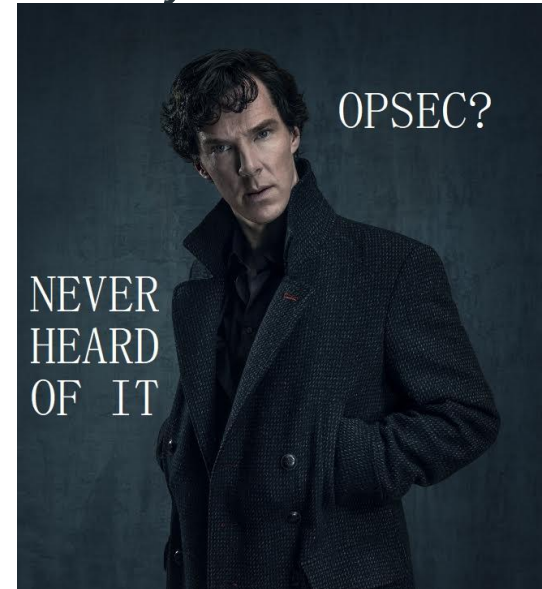
5.

OpSec? What's  
that?

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

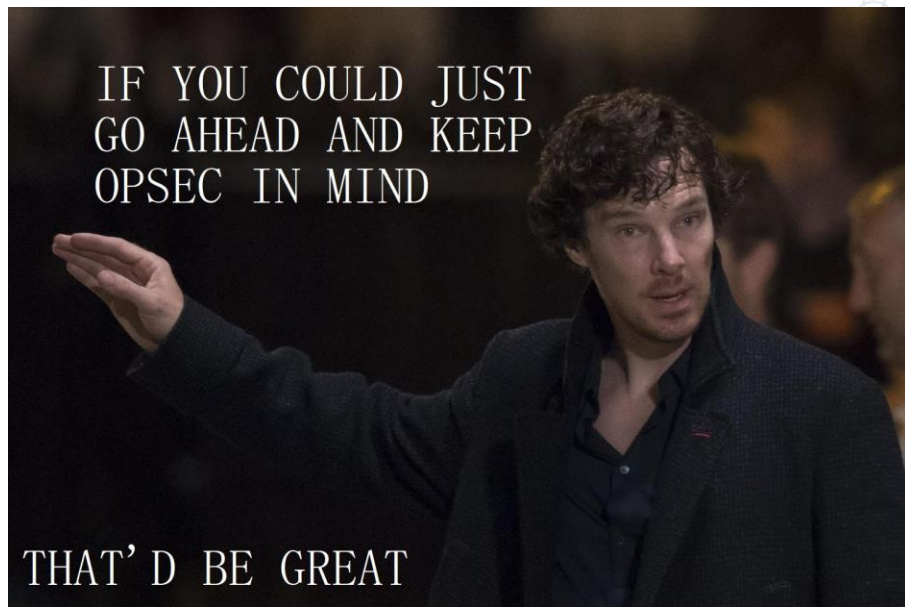
# What is OpSec?

- ◎ 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
- ◎ Never talk about your work
- ◎ Maintain different persona
- ◎ Take extensive notes
- ◎ Use password manager



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 different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

# 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 different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.



# What we discussed so far?

- ◎ Little about the Dark Web
- ◎ Dark Web forums/marketplaces
- ◎ Dark Web threat hunting
- ◎ Scrapy
- ◎ HUMINT
- ◎ Automating the Dark Web hunting
- ◎ OpSec

# If you take one thing from this talk,

- ◎ Figure out your assets
- ◎ Create hunting pipeline (Scrapy, ELK, Redis, etc.)
- ◎ Start Scrapy and put your data into ELK
- ◎ Search for your company's name in Kibana
- ◎ If found -> Analyze the results
- ◎ Do this on a monthly basis with different terms
- ◎ Report to your team through intelligence briefing

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

- ◎ Dark Web threat hunting is hard but worth the effort
- ◎ Keep OpSec in mind
- ◎ Look at more than one resource (clear web/dark web)
- ◎ Takes a lot of resources and team effort

# Resources

- ◎ Blogs & White papers by Recorded Future
- ◎ White papers by IntSights
- ◎ Blogs by Palo Alto's Unit 42
- ◎ Blogs by CrowdStrike
- ◎ White papers by Digital Shadows
- ◎ Darkweb Cyber Threat Intelligence Mining by Cambridge University Press
- ◎ Ambly the Smart Darknet Spider talk by Cytisus Eurydice (@levitannin)

# Thanks!

## Any questions?

You can contact me at:

Twitter: @ASG\_Sc0rpi0n

LinkedIn: /in/apurvsinghgautam

