

A decorative background featuring a network diagram with nodes and connecting lines, primarily in light gray, with some nodes highlighted in blue and white. The diagram is positioned in the top-left and bottom-right corners of the slide.

# 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
  - ◎ 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 the Dark Web hunting be automated?
- ◎ Overall Picture
- ◎ 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 small circles, some solid and some hollow, connected by thin lines. The overall structure is a dense, branching network.

# 1. Introduction to the Dark Web

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.

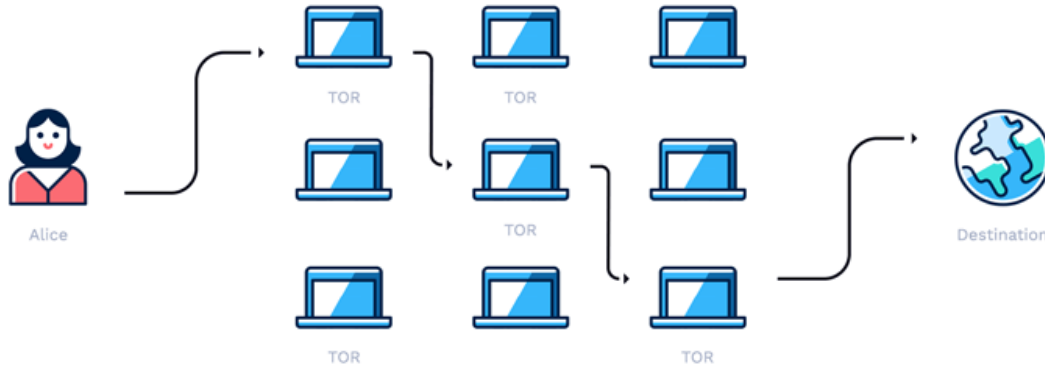
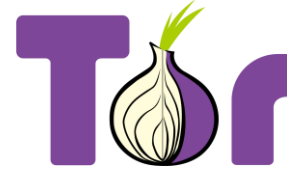
# Clear Web? Deep Web? Dark Web?



Image Source: UC San Diego Library

# Accessing the Dark Web

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



# What's all the Hype?

## ◎ Hype

- Vast and mysterious part of the Internet
- Place for cybercriminals only
- Illegal to access the Dark Web

## ◎ Reality

- Few reachable onion domains
- Uptime isn't ideal
- Useful for free expression in few countries
- Popular sites like Facebook, NYTimes, etc.
- Legal to access the Dark Web



# Relevant site types?

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

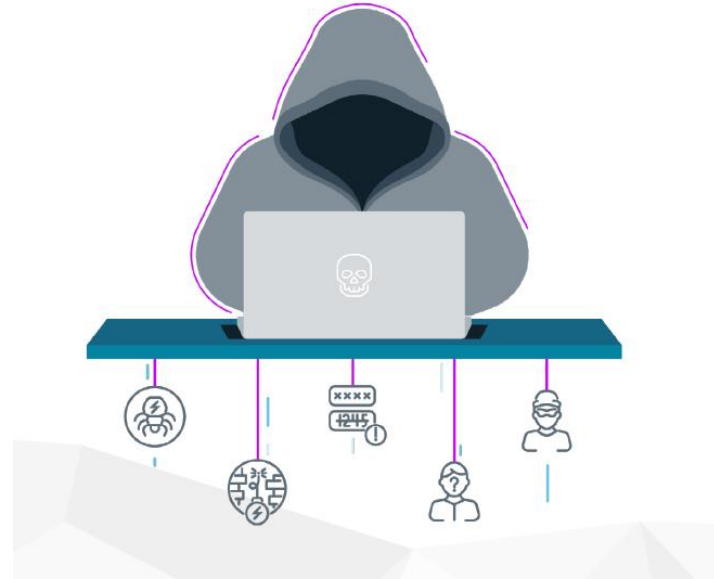


Image Source: Intsights



# Sites Examples

## Drugs

- [Drug Market](#) - Anonymous marketplace for all kinds of drugs.
- [Greenroad](#) - Biggest marketplace with full working escrow.
- [Weed&Co](#) - Weed / Cigarettes ... Prix Bas / Low Price ... weed / cigarette

## 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 Authorities of the Netherlands, listing Active, identified, and arrested Darknet M
- [Cryptome](#) - Arch on freedom of expr secret and classifi
- [SecureDrop](#) - An from and communi

## H/P/A/W/V/C

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

- [HeLL Forum](#) - HeLL Reloaded
- [RelateList](#) - New era of intellig
- [CODE: GREEN](#) - Ethical hack
- [Hack Canada](#) - America is a jc
- [Hacker Place](#) - Site with sever
- [WE fight censorship](#) - a Repor 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.

## Books

- [Example rendezvous points page](#) - Thomas Paine's *Common Sense* and *The Federalist papers*.
- [Traum library mirror](#) - 60GB of Russian and English books. A mirror of the latest Traum ISO. Covers, search and downloads in FB2, HTML and plain TXT.
- [ParaZite](#) - Collection of forbidden files and howto's (pdf, txt, etc.).
- [Jotunbane's Reading Club](#) - "All your ebooks belong to us!"
- [Liberated Books and Papers](#) - A small collection of hard to find books.
- [Clockwise Library](#) - A collection of art and science books.

# Cost of products?

- ◎ SSN - \$1
- ◎ Fake FB with 15 friends - \$1
- ◎ DDoS Service - \$7/hr
- ◎ Rent a Hacker - \$12/hr
- ◎ Credit Card - \$20+
- ◎ Mobile Malware - \$150
- ◎ Bank Details - \$1000+
- ◎ Exploits or 0-days - \$150,000+
- ◎ Critical databases - \$300,000+

# 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

## AVERAGE COST OF ONE ACCOUNT FOR DIFFERENT ONLINE SERVICES

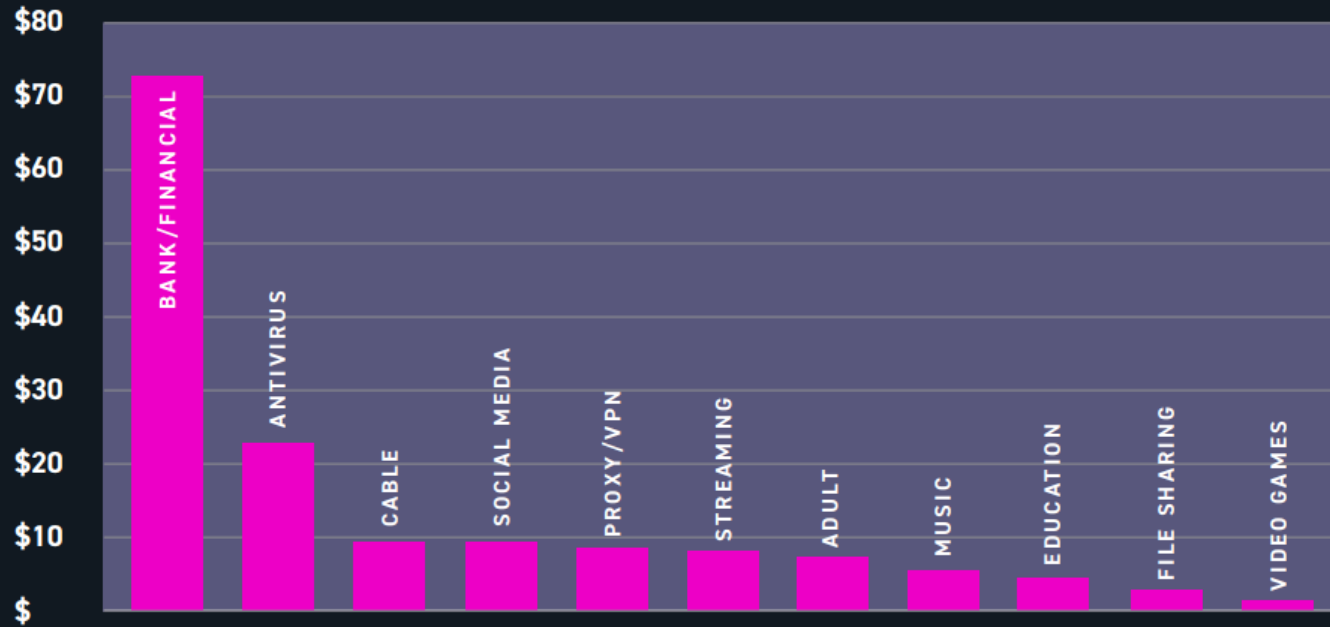


Image Source: Digital Shadows

## AVERAGE PRICES OF BRUTE-FORCING TOOLS BY TARGET INDUSTRY

**BANK/FINANCIAL**

**\$74.30**

**MULTIPACK**

**\$9.07**

**CRYPTOCURRENCY**

**\$5.64**

**SOCIAL**

**\$3.27**

**TECHNOLOGY**

**\$2.24**

**EDUCATION**

**\$0.99**

**VIDEO GAMES**

**\$0.90**

Image Source: Digital Shadows

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.

2.

## Why hunting 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. The nodes are represented by small circles, some solid and some hollow, connected by thin lines.

# What is Threat Hunting?

- ◎ Practice of proactively searching for cyber threats
- ◎ Hypothesis-based approach
- ◎ Uses advanced analytics and machine learning investigations
- ◎ Proactive and iterative search



# 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





# Benefits of Threat Hunting

- ◎ Keep up with the latest trends of attacks
- ◎ Prepare SOCs/Incident Responders
- ◎ Get knowledge of TTPs (Tactics, Techniques, Procedures) to be used
- ◎ Reduce damage and risks to the organization

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.

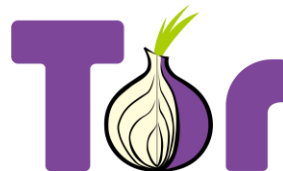
3.

# Methods to hunt on the Dark Web

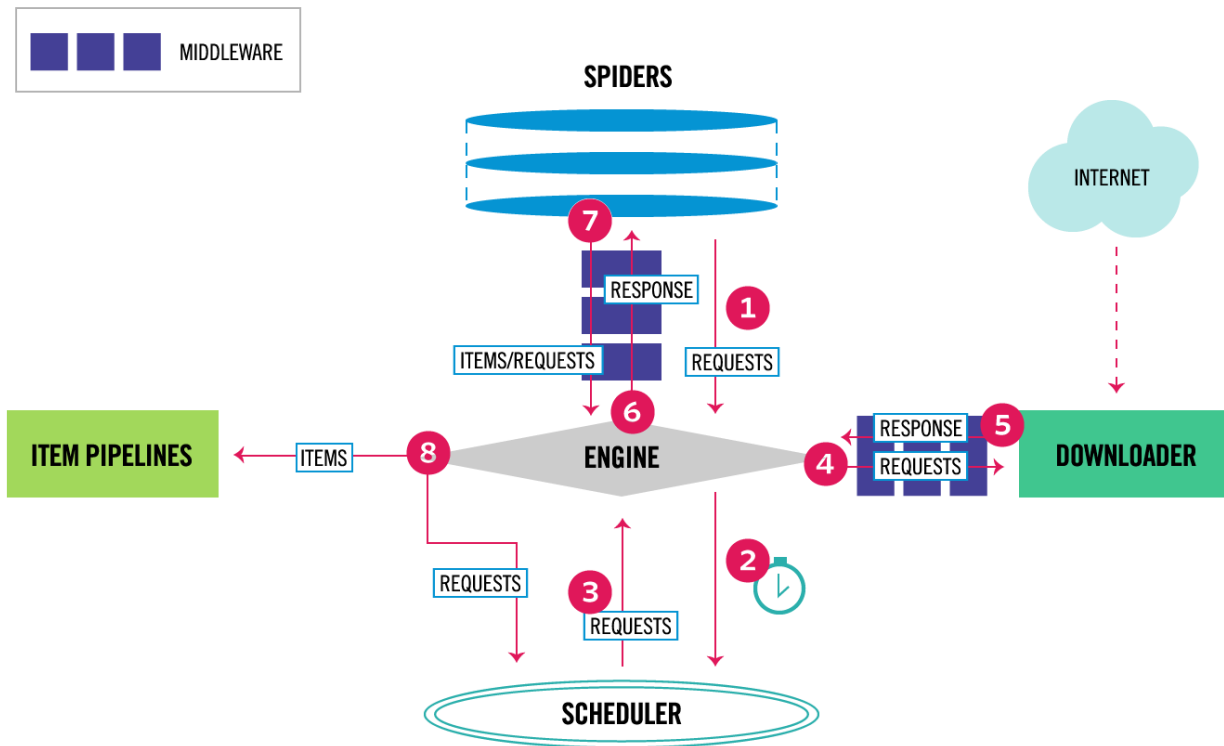
A decorative network diagram in the bottom-right corner, similar to the one in the top-left, showing a complex web of interconnected nodes and lines. The nodes are represented by small circles, some solid and some hollow, connected by thin lines.

# Tools

- ◎ Python
- ◎ Scrapy
- ◎ Tor
- ◎ OnionScan
- ◎ Privoxy
- ◎ 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

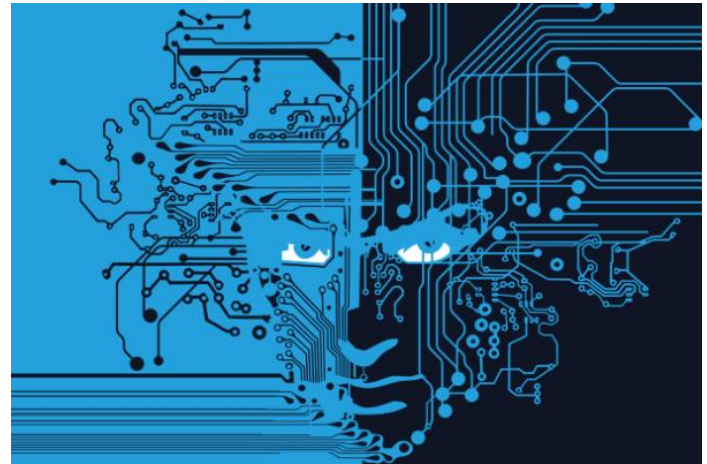


Image Source: Intsights

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

4.

**Can Dark Web hunting  
be Automated?**

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.

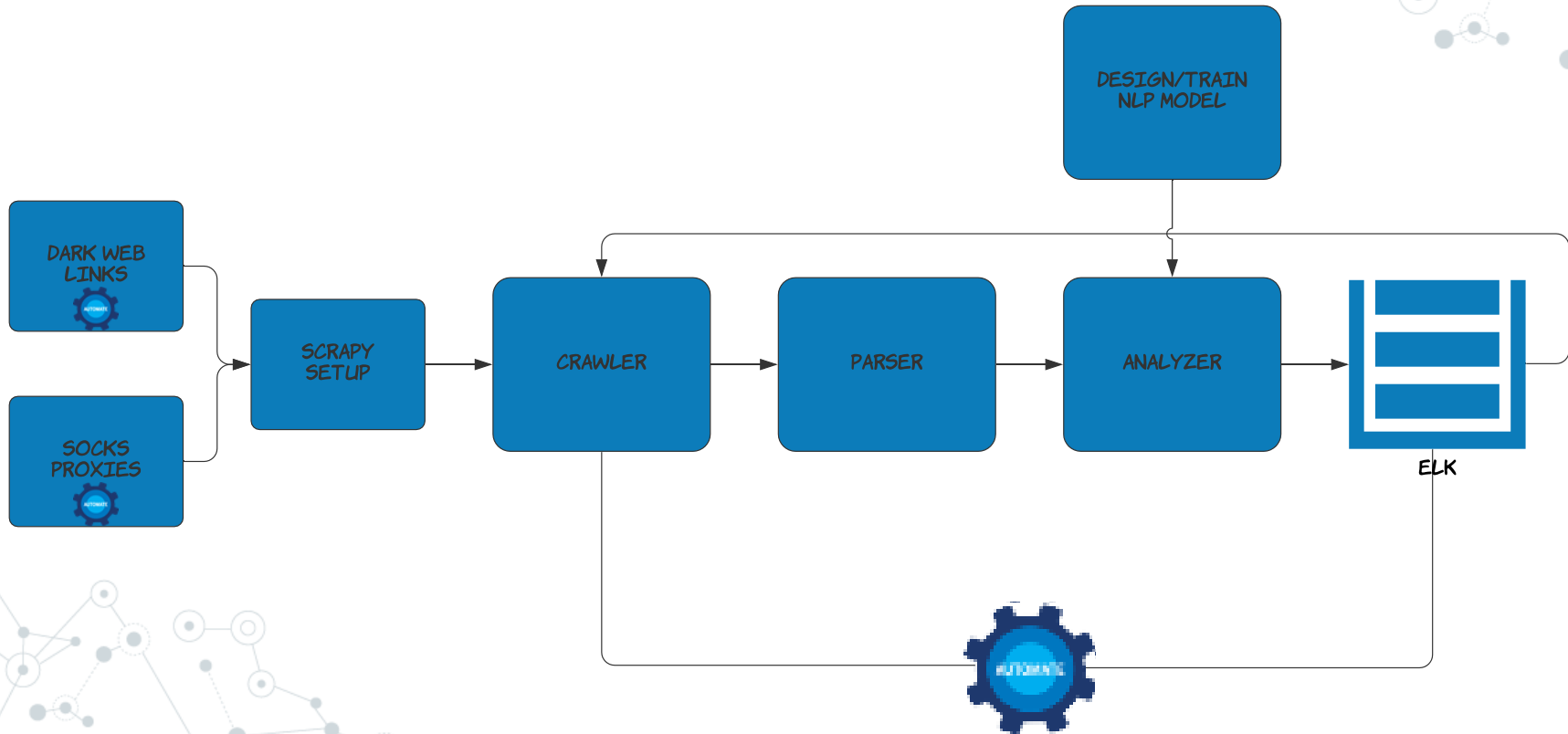
# Setting up TH Lab

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



Image Source: Hayden James

# Automated Hunting Architecture



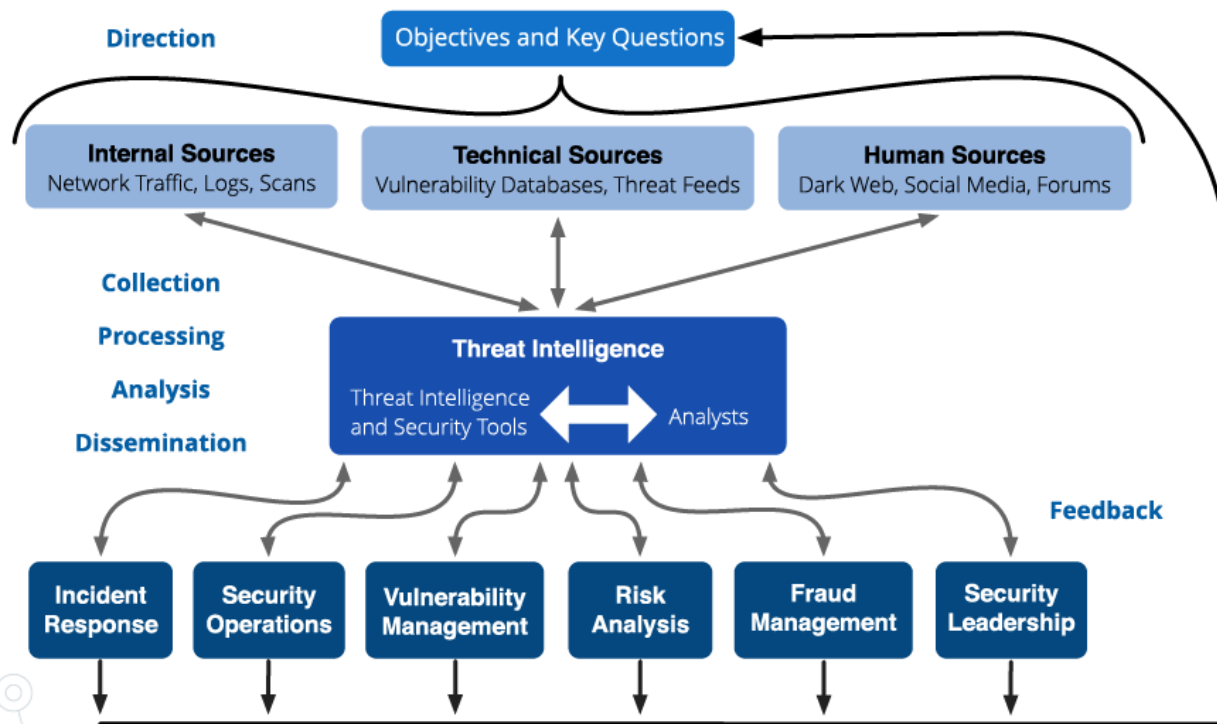


A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or central structure. The lines are thin and gray, connecting the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

# 5. Overall Picture

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 being larger and more prominent than others, indicating a central or hub-like node within the network.

# Let's talk about TI Lifecycle



# Threat Modelling

- ◎ “works to identify, communicate, and understand threats and mitigations within the context of protecting something of value” – OWASP
- ◎ Define critical assets
- ◎ Understand what attackers want
- ◎ Threat actor capability and intent
- ◎ Sources to target

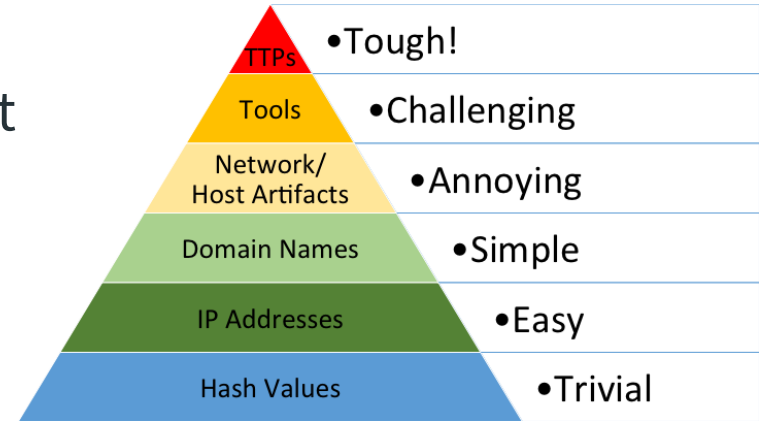


Image Source: David Bianco

# Data Collection/Processing

- Collecting data from clear web
  - Pastebin
  - Twitter
  - Reddit
  - Telegram
- Collecting data from dark web
  - Forums
  - Markets

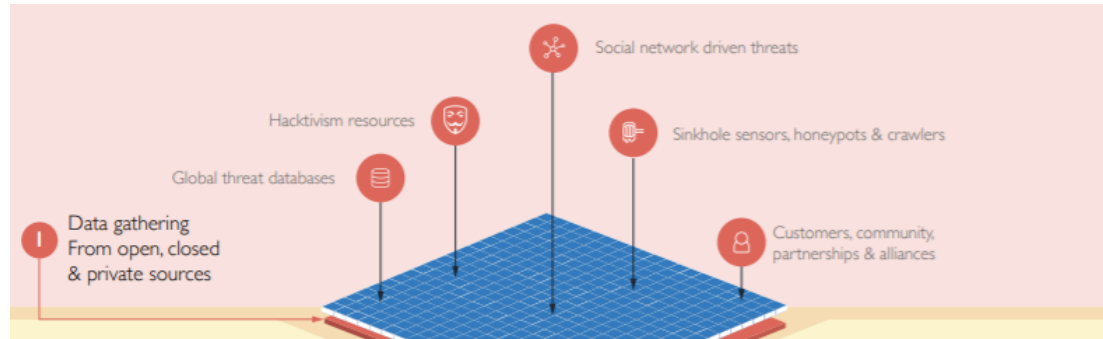


Image Source: Blueliv

# Data Analysis

- ◎ NLP/ML/DL techniques
- ◎ Social network analysis
- ◎ Classification
- ◎ Clustering
- ◎ MITRE ATT&CK



Image Sources: DataCamp, MITRE ATT&CK



6.

# OpSec? What's that?



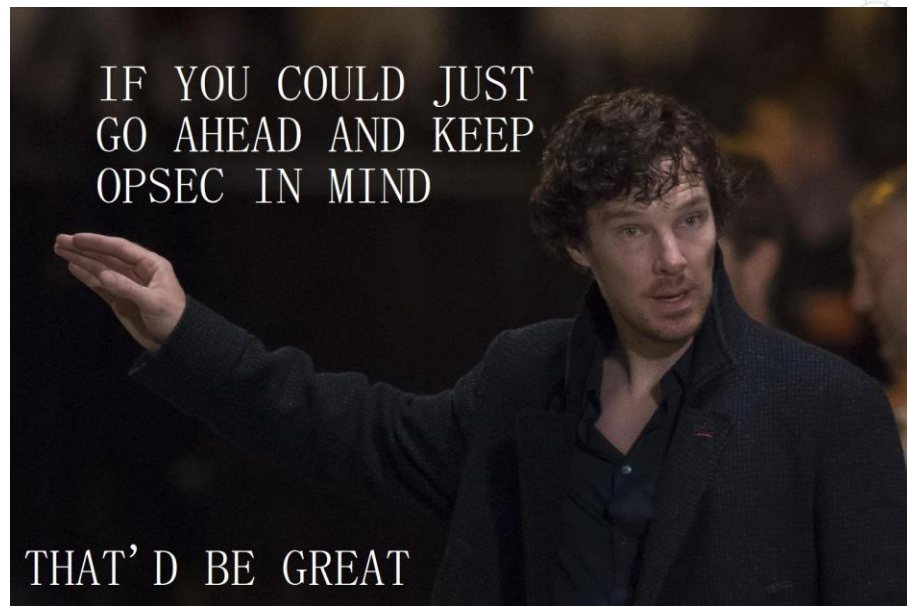
# What is OpSec?

- ◎ 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.

# 7. 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
- ◎ Little about threat intelligence lifecycle
- ◎ OpSec

# 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
- ◎ Takes a lot of resources and team effort
- ◎ Usage of MITRE ATT&CK framework

# 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

# Thanks!

## Any questions?

You can contact me at:

Twitter: @ASG\_Sc0rpi0n

LinkedIn: /in/apurvsinghgautam

