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

1.
Introduction to the Dark Web

Clear Web? Deep Web? Dark Web?

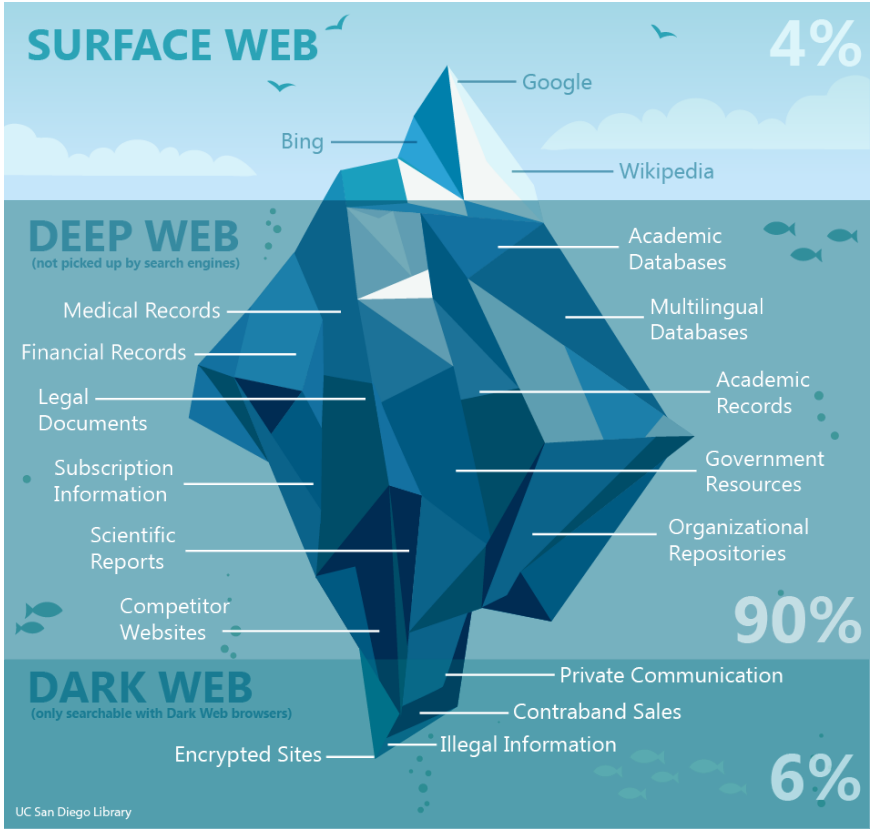
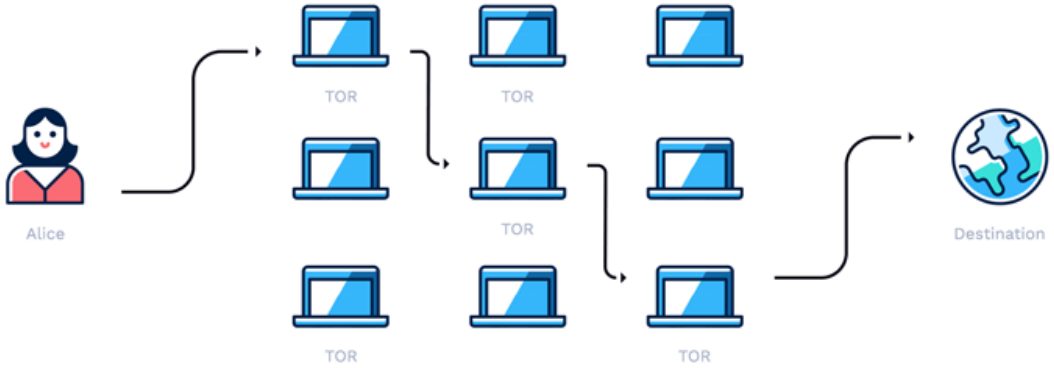


Image Source: UC San Diego Library

Accessing the Dark Web

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



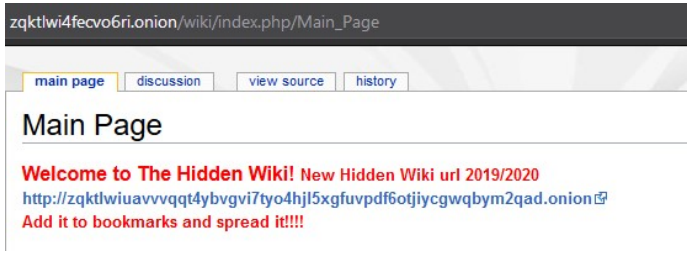


Image Sources: Hotspot Shield, Tor Project, I2P Project, ZeroNet

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

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.

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 is back!
- RelateList - New era of intellig
- CODE: GREEN - Ethical hack
- Hack Canada - America is a jo
- Hacker Place - Site with sever
- WE fight censorship - a Repor information.

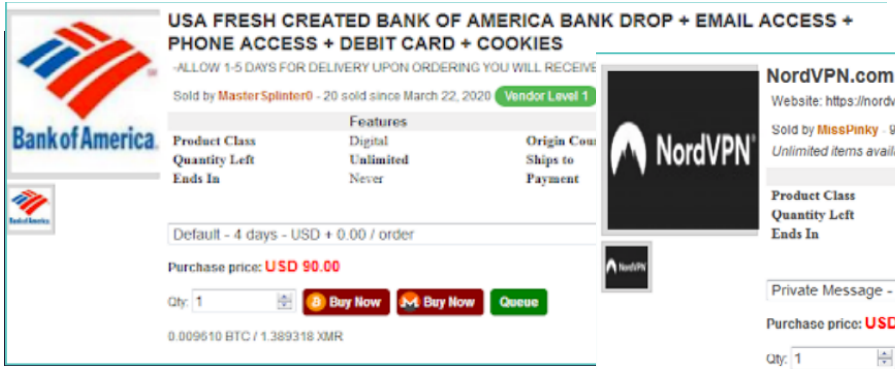
Books

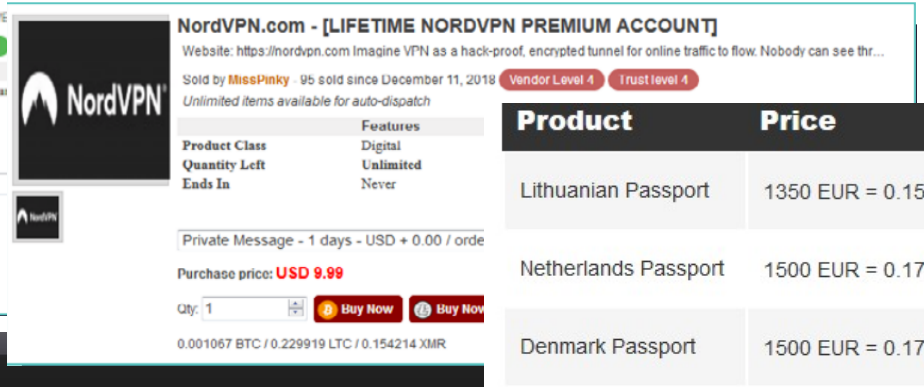
- Example rendezvous points page - Thomas Paine's *Common Sense* and *The Federalist papers*.
- Traum library mirror - 60GB of Russian and English books. A mirror of the latest Traum ISO. Covers, search and downloads in FB2, HTML and plain TXT.
- ParaZite - Collection of forbidden files and howto's (pdf, 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?

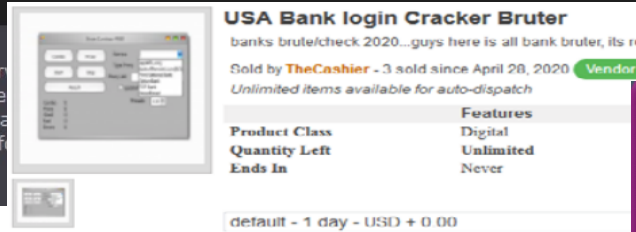
- SSN - $1
- Fake FB with 15 friends - $1
- DDoS Service - $7/hr
- Rent a Hacker - $12/hr
- Credit Card - $20+
- Mobile Malware - $150
- Bank Details - $1000+
- Exploits or 0-days - $150,000+
- Critical databases - $300,000+

Product Examples





Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.15780 Ƀ	1 X Buy now
Netherlands Passport	1500 EUR = 0.17533 Ƀ	1 X Buy now
Denmark Passport	1500 EUR = 0.17533 Ƀ	1 X Buy now
	Ƀ	1 X Buy now
	Ƀ	1 X Buy now



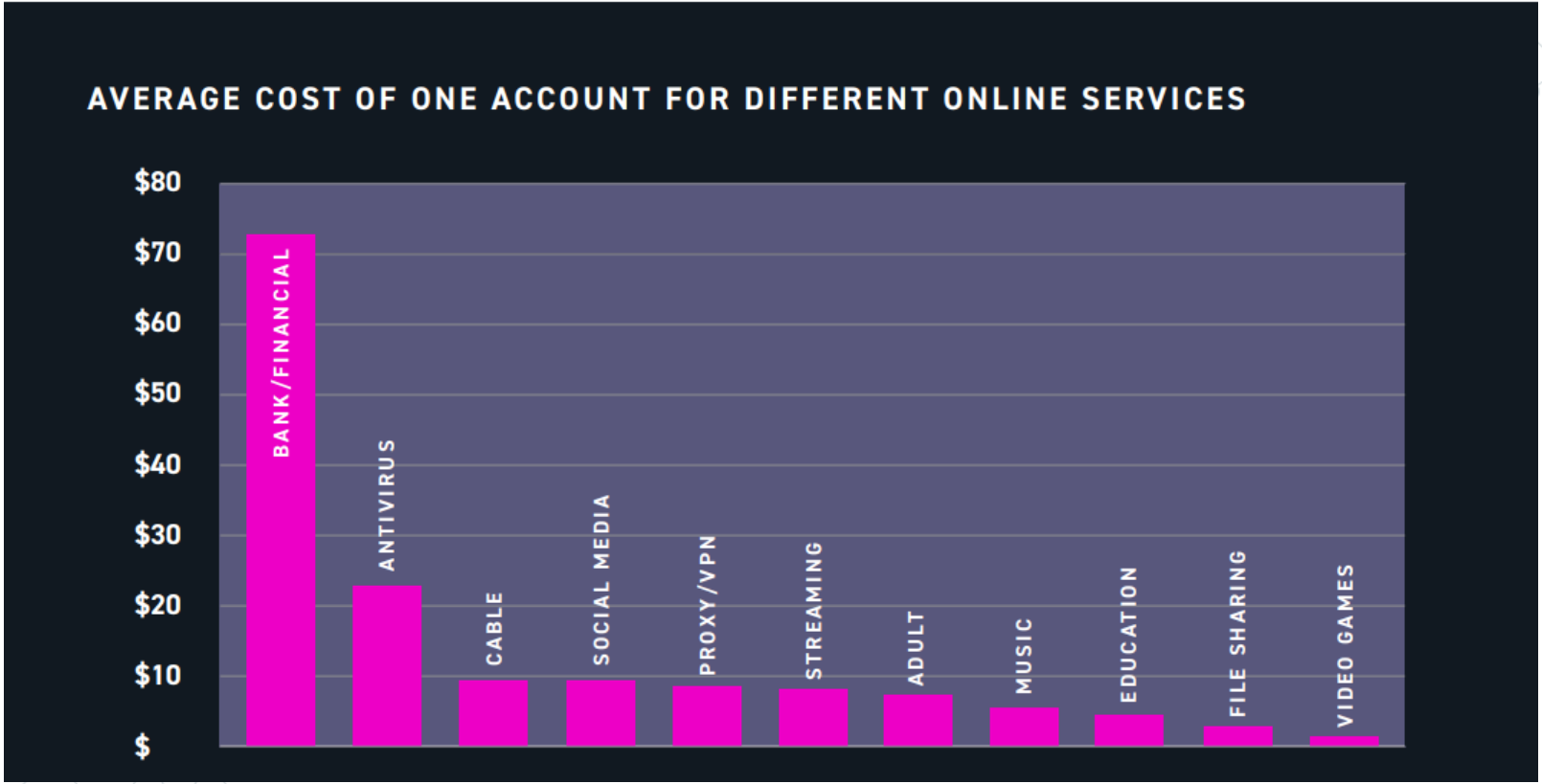


Image Source: Digital Shadows

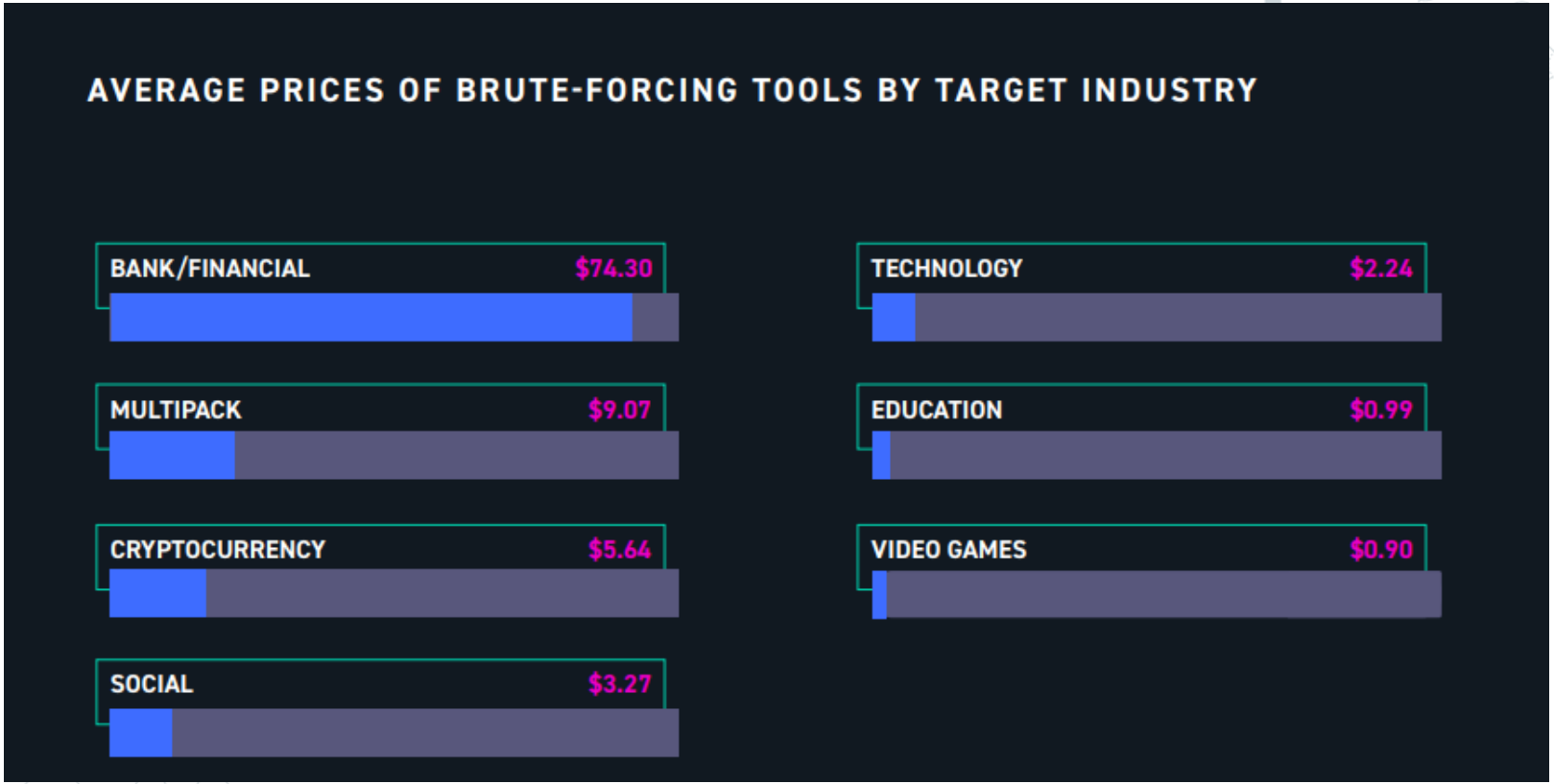
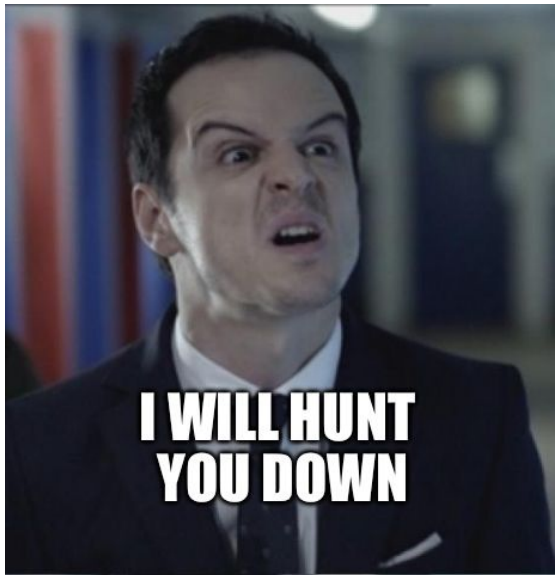


Image Source: Digital Shadows

2.
Why hunting on the Dark Web

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

3.
Methods to hunt on the Dark Web

Tools

- Python
- Scrapy
- Tor
- OnionScan
- Privoxy
- and many more…

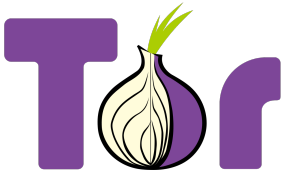


Image Sources: Tor Project, OnionScan, Python, Scrapy, Privoxy

How Scrapy Works?

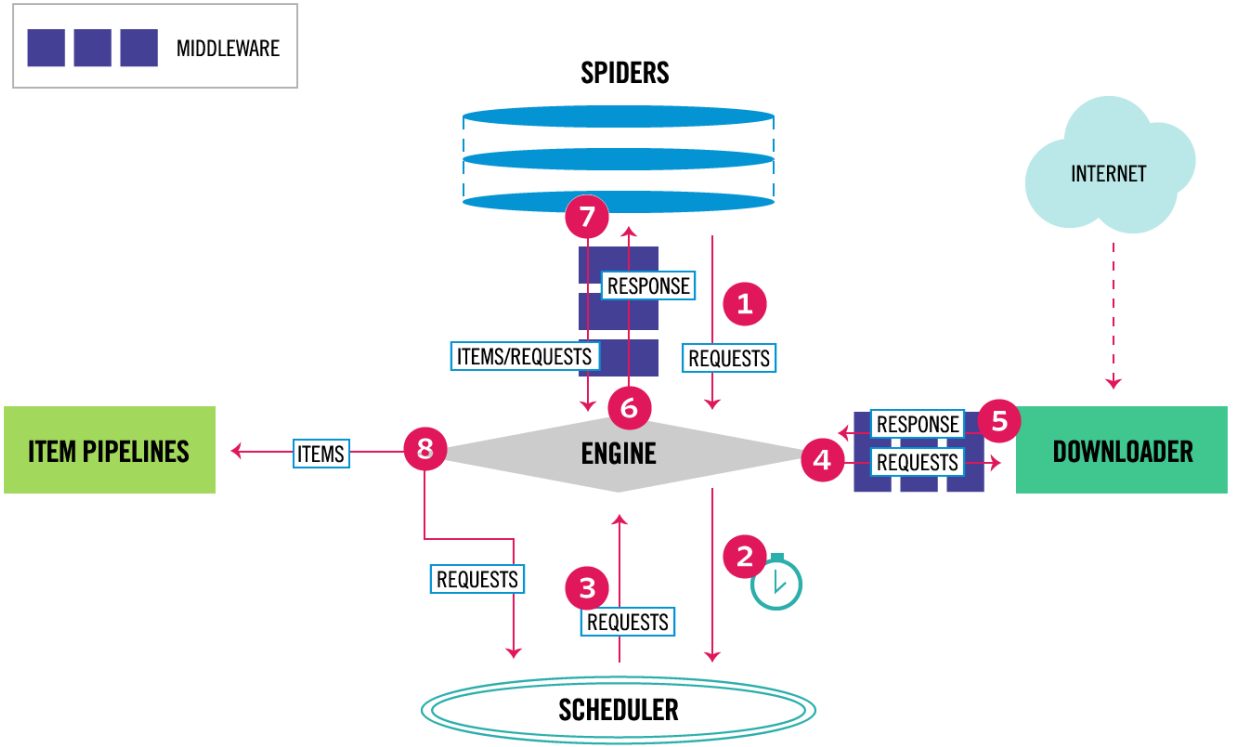


Image Source: Scrapy Docs

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

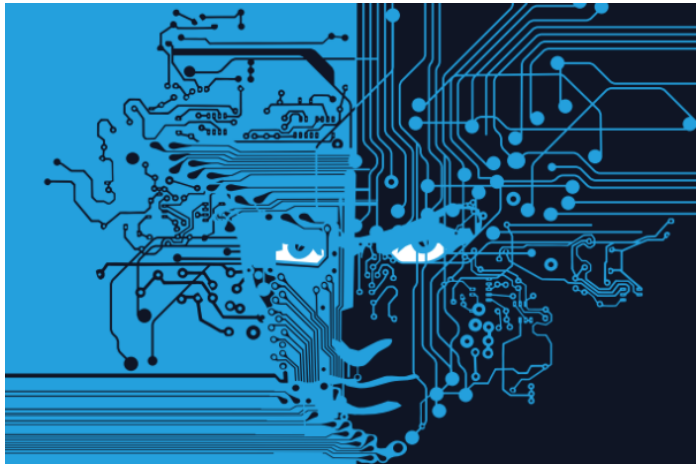


Image Source: Intsights

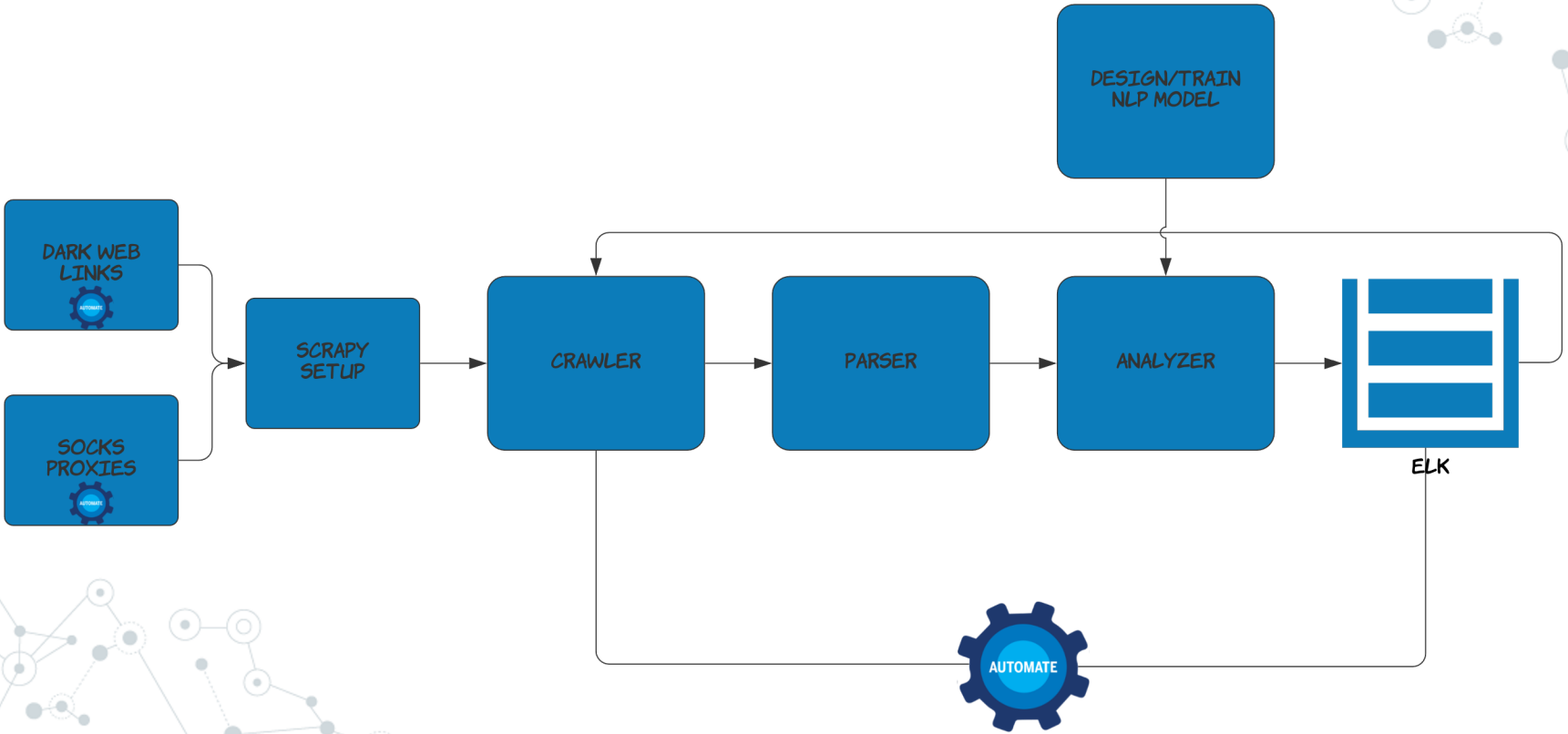
4.
Can Dark Web hunting be Automated?

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



5.
Overall Picture

Let’s talk about TI Lifecycle

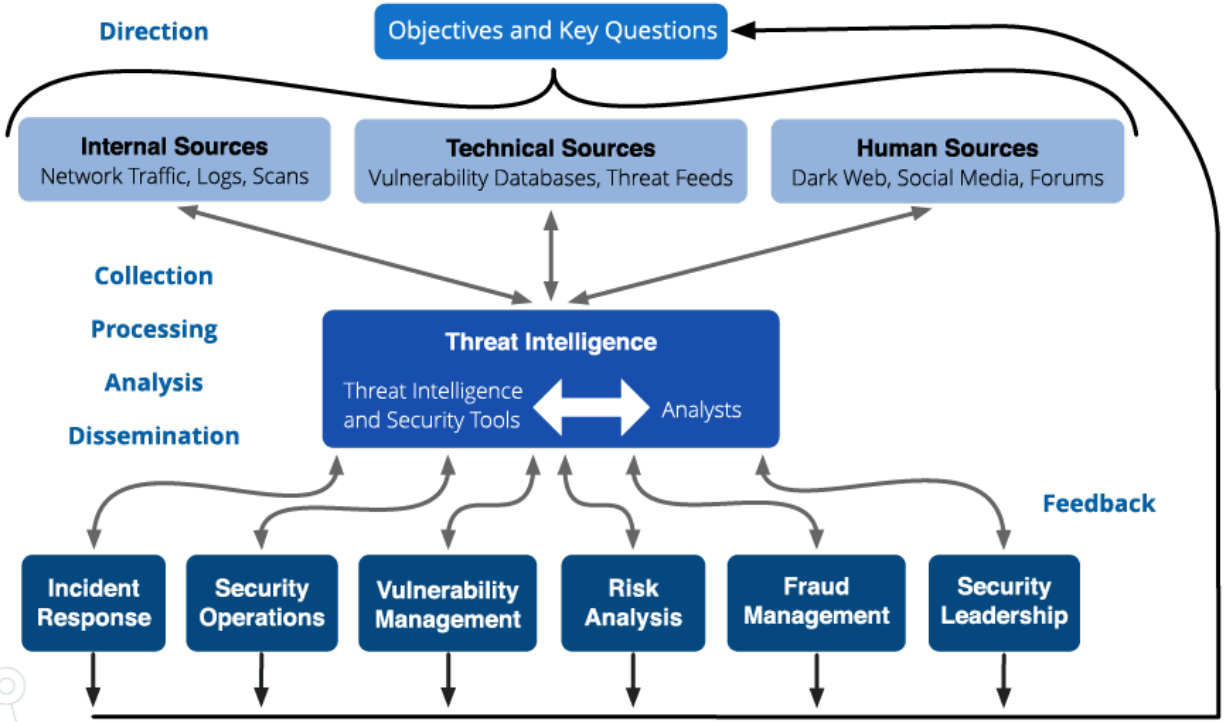


Image Source: Recorded Future

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

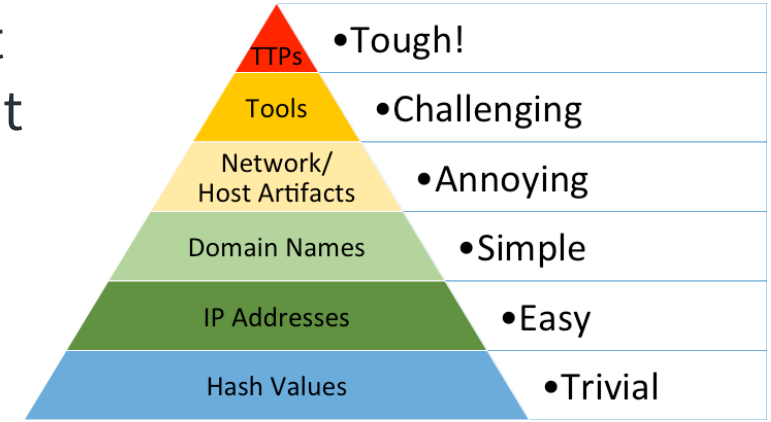


Image Source: David Bianco

Data Collection/Processing

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

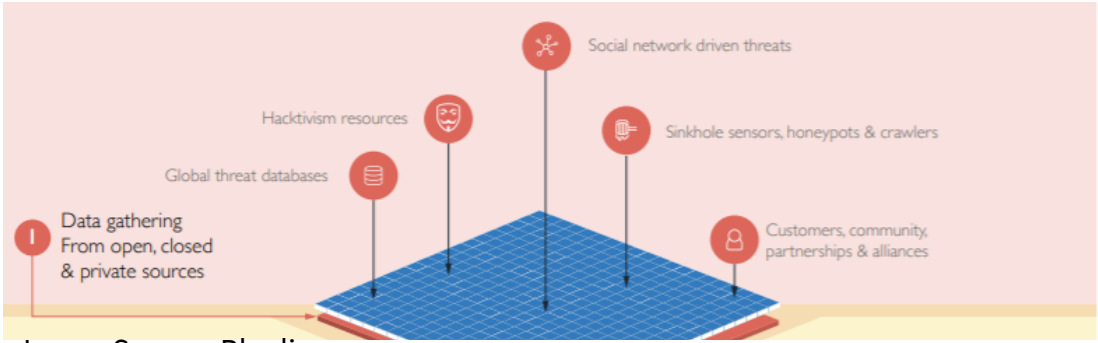


Image Source: Blueliv

Data Analysis

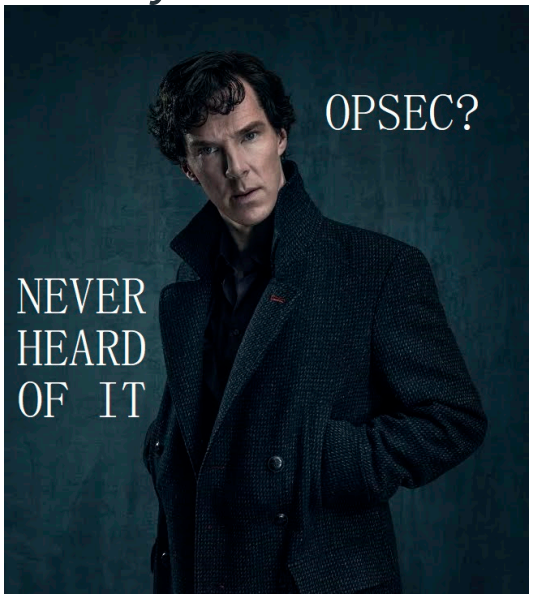
- NLP/ML/DL techniques
- Social network analysis
- Classification
- Clustering
- MITRE ATT&CK

Image Sources: DataCamp, MITRE ATT&CK

6.
OpSec? What's that?

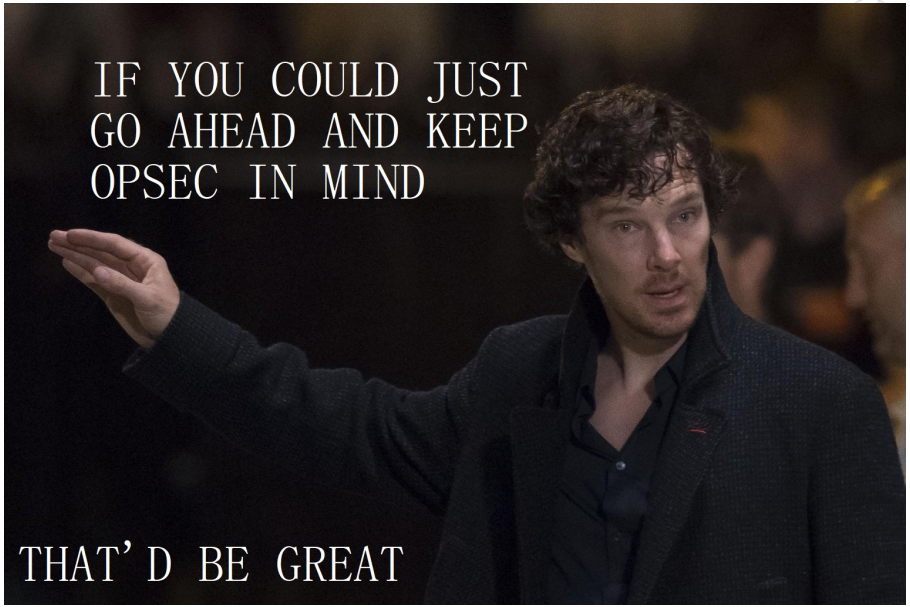
What is OpSec?

- 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



7. Conclusion

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