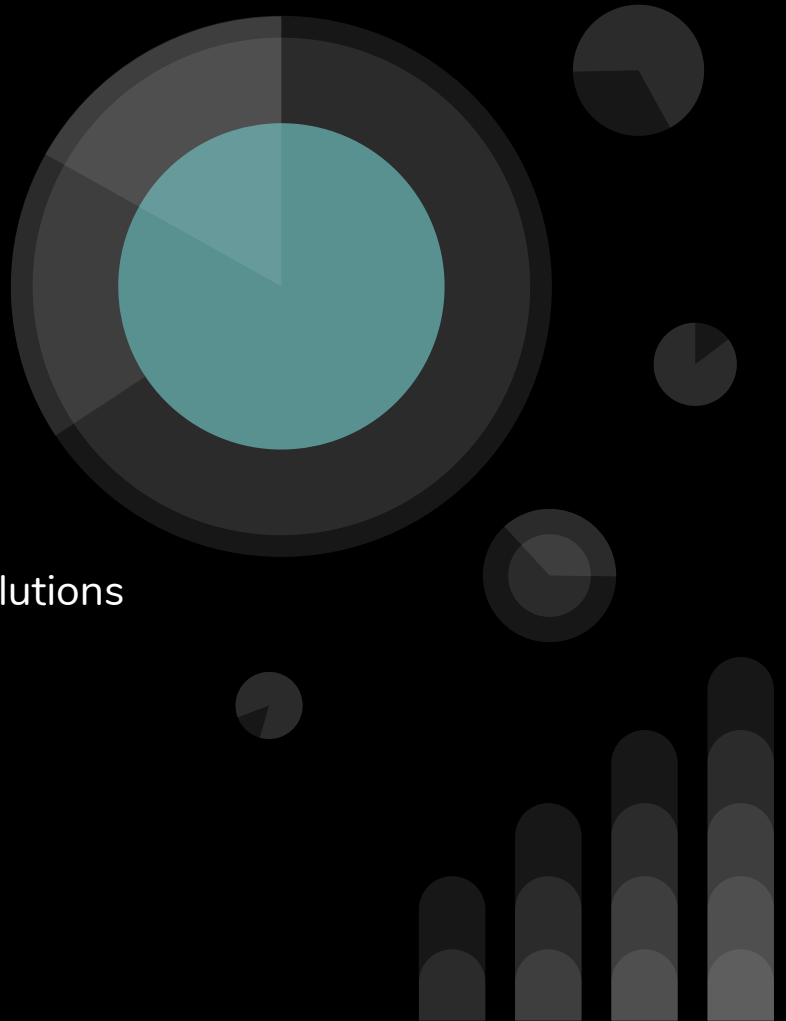
Anonymous Networks

F Latif, Z Liu, S Johal

Overview



- What is an anonymous network ?
- Motivations for anonymous networks
- Examples of anonymous networks
- Attacks on Anonymous network and solutions
- How is it misused in business ?

Anonymous Networks: An Introduction

- Anonymous networks are created by softwares that encrypt traffic and hide identities(IP addresses, names, nationality, etc.)
- Are mostly P2P
- Built on top of the Internet and its standard layers
- Darknet refers to the sum of all the anonymous networks that operate
- Examples of anonymous networks:
    - TOR(The Onion Routing), I2P(Invisible Internet Project), Freenet

Anonymous Networks: History and Motivation

- Created from a need of a network privacy and security.

- Desired features for anonymization:
  - Hide IPs, hide browser fingerprint, minimize or stop use of cookies, and so on.

- Individuals use the darknet for:
  - Almost any criminal activity
  - Prosecutable actions such as human rights advocacy, whistle blowing and journalism.


How are anonymous networks possible?

VPN

VPN = Anonymous network

Any trusted VPN service is good enough to get anonymity.
Users stay anonymous and cannot be tracked due to the layered encryption system.

How does a VPN work?

- VPN creates an encrypted connection or tunnel between your device and the Internet.
- During the tunneling process, your IP address changes to the VPN server address.
- This IP address is assigned to thousands of other users of the VPN service and the result is that your online activities cannot be traced.

VPN alone can't provide anonymity

- the VPN has to be trusted to encrypt traffic
- cookies and other details may not be taken care of

IPSec

VPN is implemented over IPSec. **-> The connection is created over IPSec**

1. Provides cryptographically-based security to network traffic.
2. Provides security to routers routing data over the internet
3. Creates the virtual, encrypted link over the unsecured network.

Surface Web / Public Web :

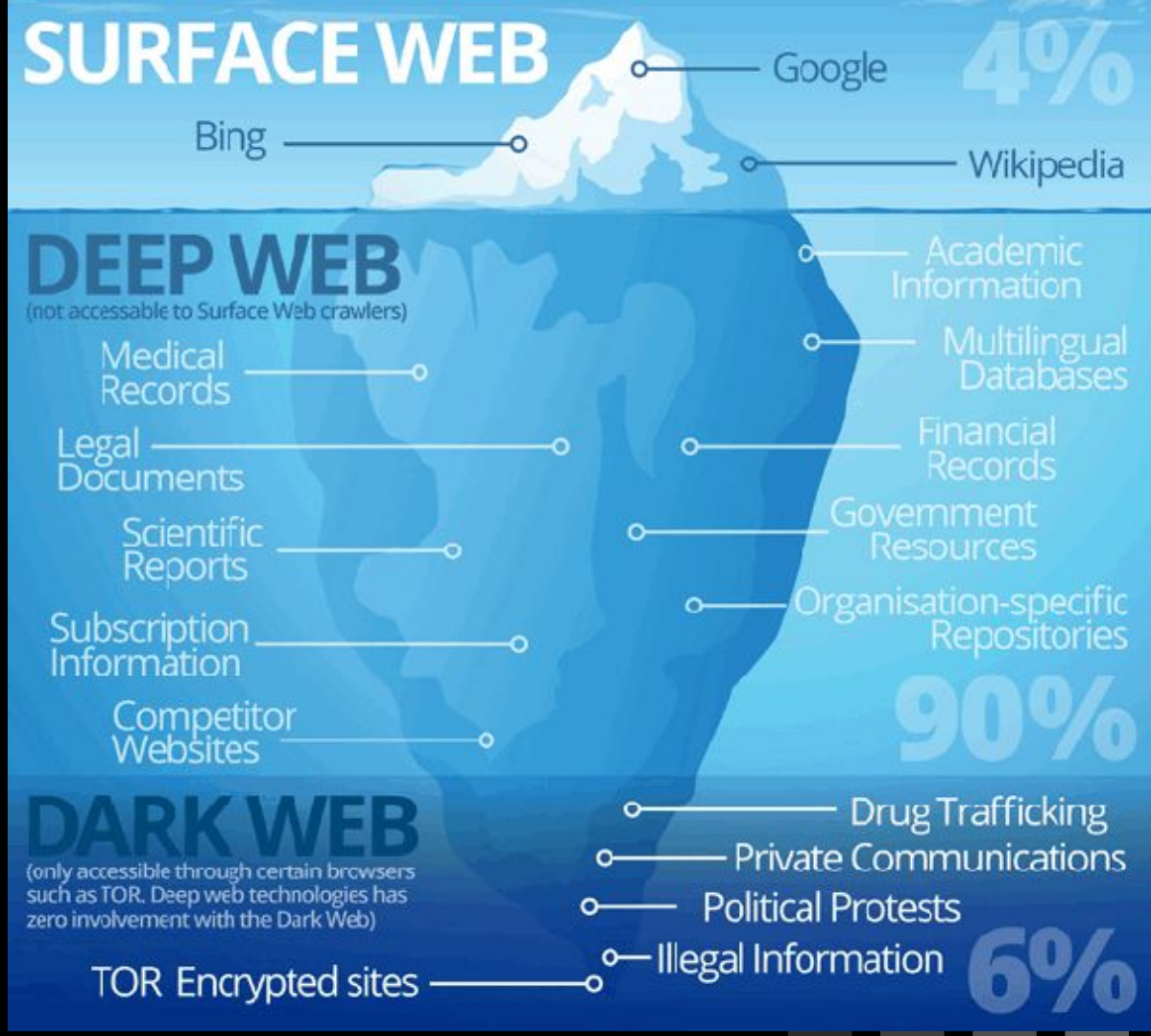
- what we see

Deep Web:

- Classified and private data
- Archives, documents, records
- Can’t be accessed by search engines

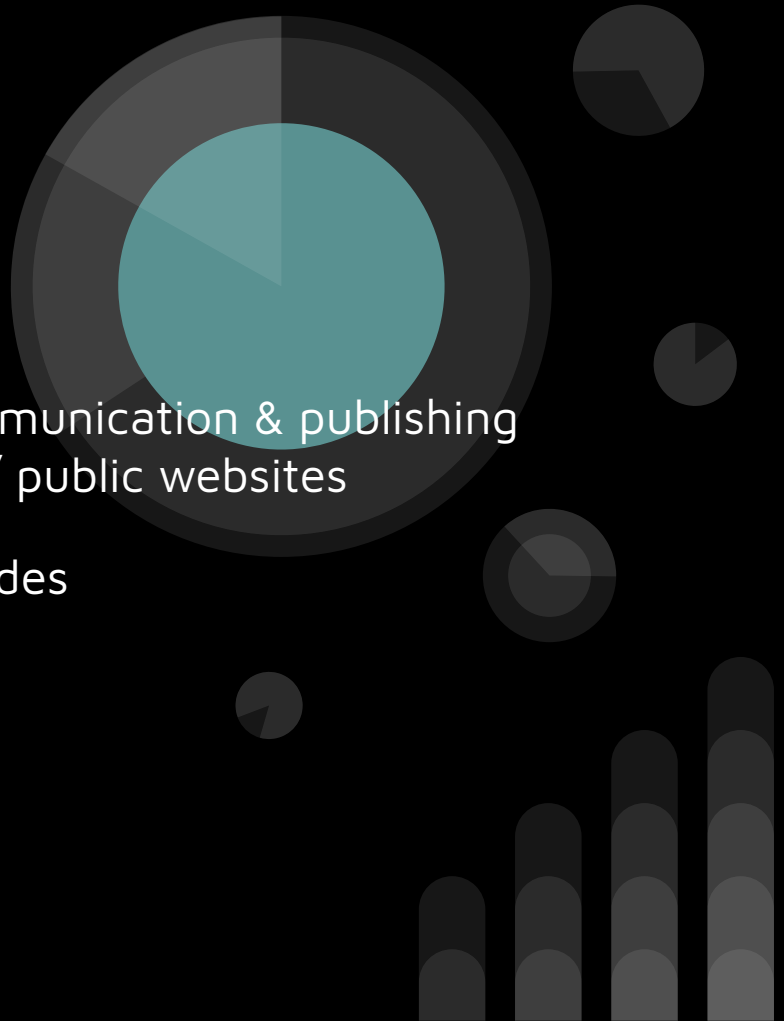
Dark Web:

- Blackmarket of the web
- Specific browsers and softwares are needed to access it

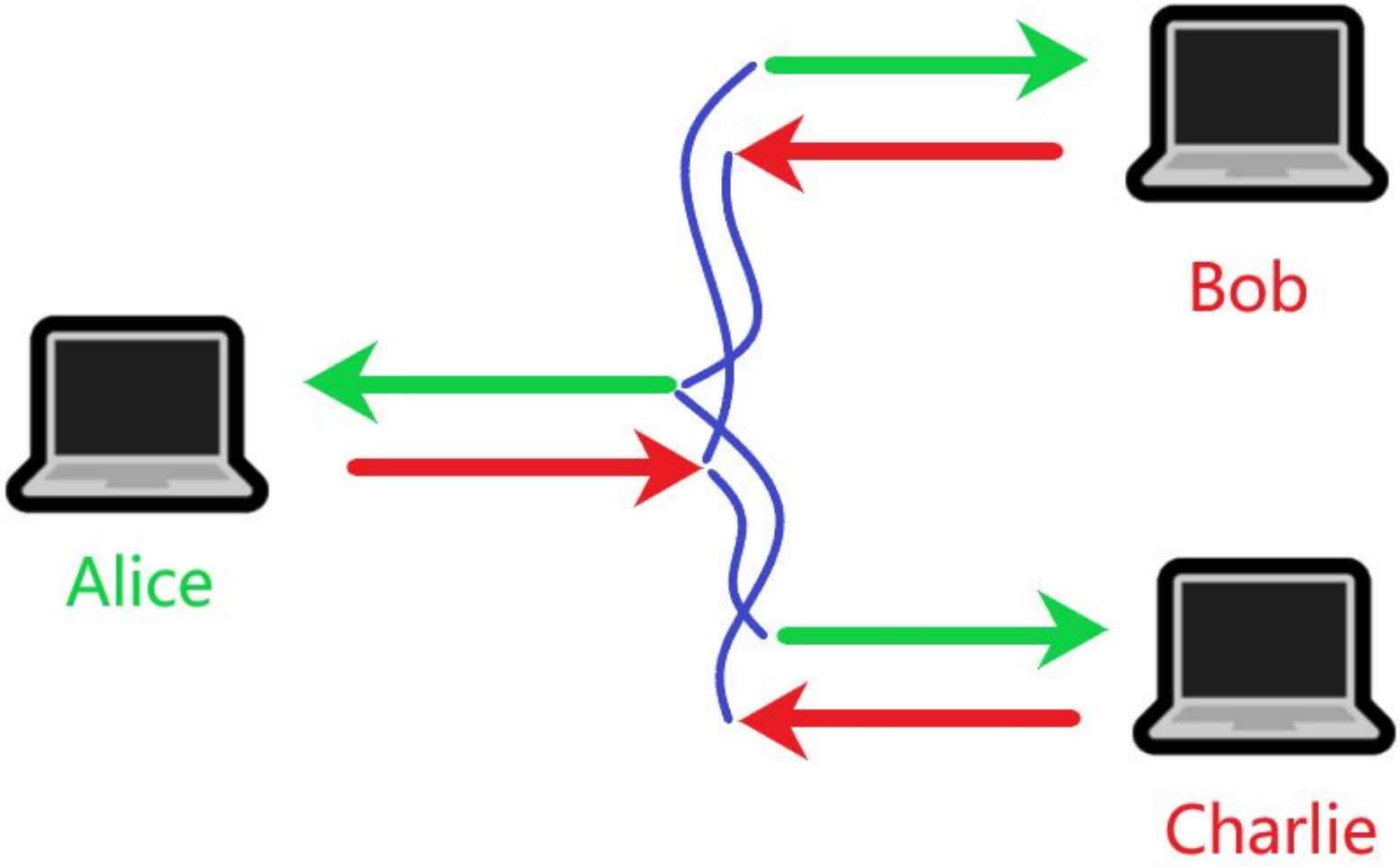


Freenet & I2P

The Invisible Internet Project



- Peer to peer platform for uncensored communication & publishing
  - Anonymously share files and browse / public websites
- Freenet: communication via encrypted nodes
- I2P: Tunnels for communication


Bob
Alice
Charlie

TOR - The Onion Routing

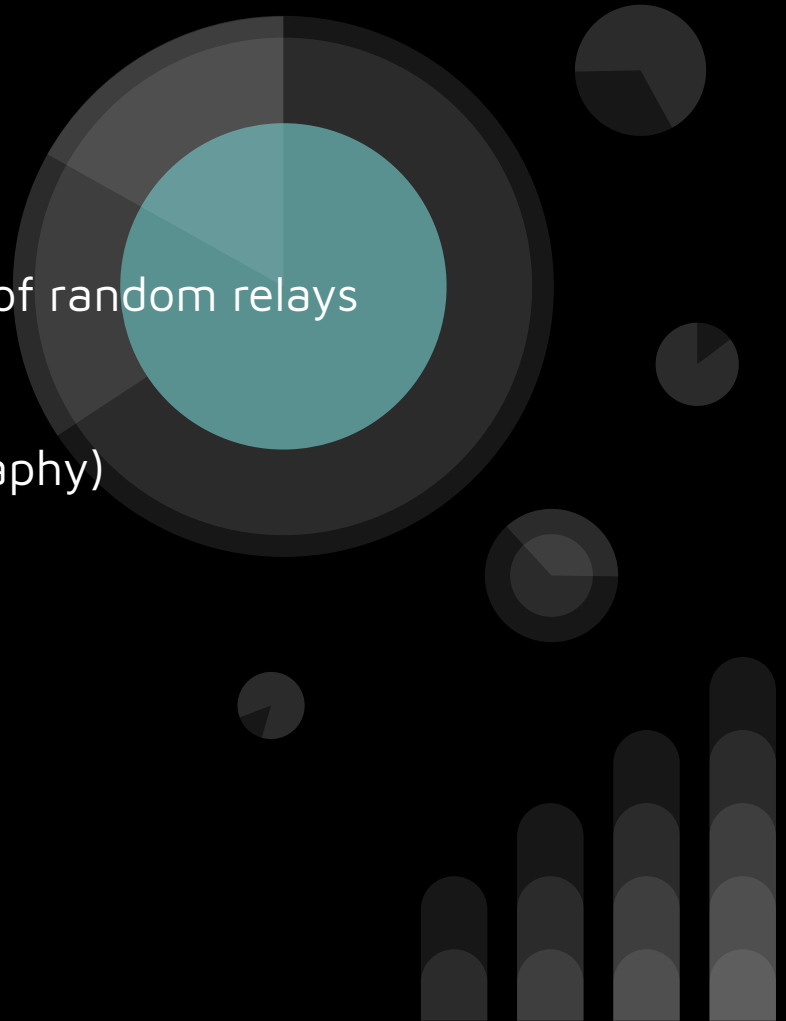
- Onion routing concept since 1990s → Developed by US Navy in 2000s
  - More recently: Tor Browser

- Tor Browser: Modified Firefox
  - Very popular due to being free & simplicity of operation
  - To protect privacy and grant unrestricted access

- Traffic Analysis protection
  - Discrimination based on locality
  - Threat to personal safety

Onion Routing

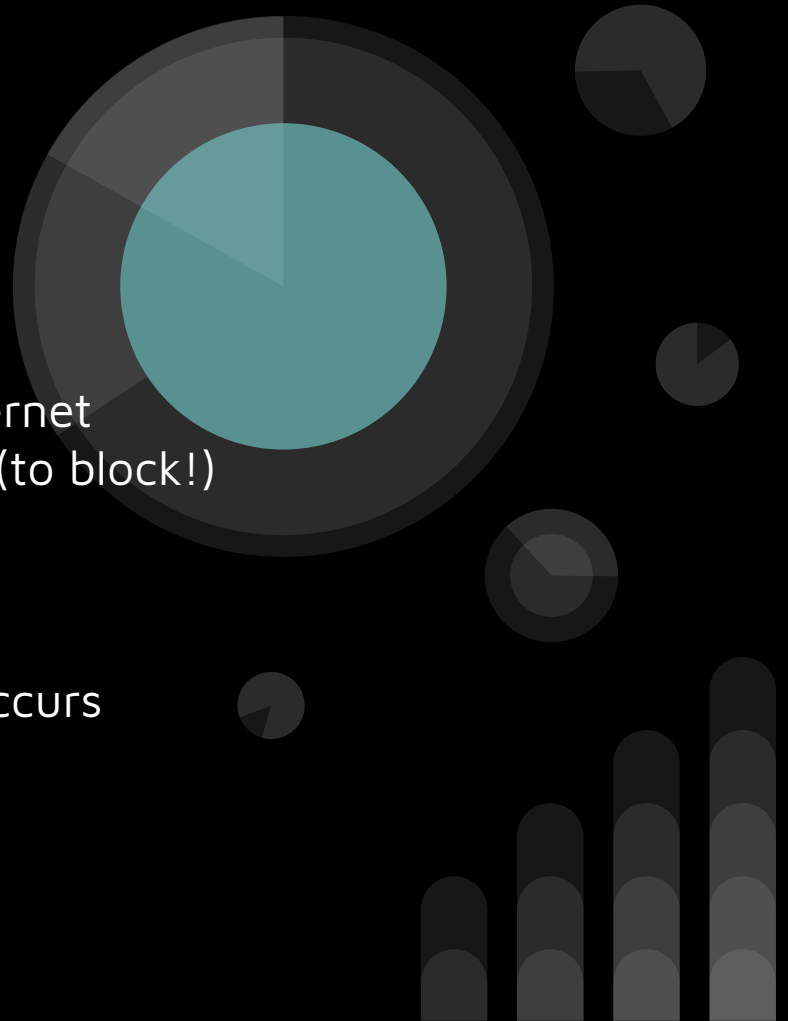
- Routes user internet traffic through a set of random relays
  - Volunteer nodes
- Data is encrypted (Elliptic Curve Cryptography)
  - Resistant to brute-force attacks
- Encrypted data is passed through relays
  - Entry / Guard Relays
  - Middle Relay
  - Exit Relay




Tor Node
Encrypted
Unencrypted


Tor Node
Encrypted
Unencrypted

Onion Routing



- Relays are all publicly available on the internet
  - Can be targeted by ISPs/government (to block!)

- Bridges: non-public relays
  - Private: cannot be blocked
  - Utilized in countries where blocking occurs

Attacks on Anonymous Networks

TOR DoS: Cell Attack

Objective: Cause an onion router to drop packets of its routes/circuits.

Method: The attacker keeps adding an onion router to their onion circuit/route for transmitting packets. The victim starts dropping its packets as the attacker makes too many requests.

The work ratio between the sending the request and processing it is 20:1.

The CPU cannot send packets and handle the requests.

Defense: Make the attacker solve cryptographic puzzles to slow down their request rate, reducing the node's CPU usage, adjust the puzzles' difficulty for circumstances. Lower the 20:1 ratio.

TOR DoS: Sniper Attack

Objective: Crash TOR routing software on entry or exit nodes' with memory overflow.

3 versions of the attack characterized by what the attacker controls and efficiency.

The attacker sends or requests packets using TOR and then stops receiving responses. Refusing to receive packets builds queues. These crash TOR on the node a with memory overflows.

Defense: When memory runs low, drop TOR circuits/connections according to FIFO order.

TOR Deanonymize: Repeated Sniper Attack

Objective: Get info on clients from their IP Headers

Repeat the sniper attack to crash border nodes until the attacker’s onion router node is randomly selected to be their replacement guard node.

Defenses: Be more demanding when picking guards and limiting the rate of replacement selection.

TOR Deanonymize: End to End Timing Attacks

Objective: Match encrypted traffic from the source address to the destination address.

Requirements: The attacker needs to sniff packets going into the TOR entry nodes and out of the TOR exit nodes.

Find patterns in packets' sizes and timings so the attacker knows who is communicating with who, using TOR.

Defense: Sequences of packets are sent using different TOR circuits(routes) and delay packets to sabotage traffic's timing analysis

How is it misused in business ?

- ★ E-commerce:
  - Frauds with stolen credit card use anonymous network to :
    - Spoof locations close to the billing or shipping addresses of the victim [same to how spam callers spoof phone's area code]
- ★ Media streaming:
  - Consumers use to bypass geolocation controls and get contents not available in their area
- ★ Dark web:
  - Blackmarket of the web
  - Revenue: **~ in billions per year**
  - User: **~ millions around the world**
  - Uses innovations of legitimate e-commerce sites like Amazon or eBay.
  - It has become a hub for certain illegal economic activities.
  - Certain good tasks also happen here. Like journalism, blogging in a restricted country.

Cannabis	31.60%
Pharmaceuticals	21.05%
MDMA	10.53%
LSD	5.26%
Meth	5.26%
Mushrooms	5.26%
Heroin	5.26%
Seeds	5.26%
Video games	5.26%
Accounts	5.26%

Vendor breakdown based on data pulled on 3 June 2015

Cannabis	27.28%
Pharmaceuticals	22.39%
MDMA	14.43%
LSD	7.47%
Meth	3.93%
Mushrooms	3.41%
Heroin	3.31%
Seeds	3.92%
Video games	6.93%
Accounts	6.93%

Buyer breakdown based on data pulled on 3 June 2015

Thank you everyone

References

- http://cryptowiki.net/index.php?title=Anonymity_networks
- https://www.codeproject.com/Articles/1205964/Design-and-develop-an-Anonymous-network
- https://www.radware.com/newsevents/mediacoverage/anonymous-networks-101-heart-of-darknet
- https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html
- https://www.vpnmentor.com/blog/web-anonymity/
- https://www.geeksforgeeks.org/ip-security-ipsec/
- https://www.geeksforgeeks.org/deep-web-dark-web-darknet
- https://en.wikipedia.org/wiki/Darknet
- https://blokt.com/guides/browser-fingerprinting
- freenetproject.org/pages/about.html
- geti2p.net/en/about/intro
- www.torproject.org
- www.torproject.org
- http://www.nsl.cs.columbia.edu/papers/2013/cellflood.esorics13.pdf
- https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses
- https://pdfs.semanticscholar.org/1aac/5be6c8cec71afd8b9514fefe5c4aca906502.pdf
  https://blog.maxmind.com/2019/01/24/types-of-anonymous-ips-and-how-they-affect-your-business/
- https://www.investopedia.com/terms/d/dark-web.asp
- https://digital.com/blog/deep-dark-web/