

DEMYSTIFYING THE DARK WEB

JOHNNY XMAS
SR. SECURITY RESEARCHER
&
SR. TRAINER
SMFS, INC. (GRIMM)

GRIMM

[HTTPS://GRIMM.R1P](https://grimm.r1p)

JOHNNY XMAS



PREVIOUS PROFESSIONAL ROLES:

- Network Engineer
- Systems Engineer
- Information Security Engineer
- Information Security Consultant
- Penetration Tester
- OT Researcher
- Blade Runner (Bot Killer)

LINKS:

- <https://grimm.rip>
- <https://github.com/johnnyxmas>
- <https://linktr.ee/johnnyxmas>

JohnnyXmas@grimm.rip

GRIMM.rip

Sr. Security Researcher & Sr. Trainer
SMFS, Inc. d/b/a/ GRIMM

TODAY'S TOPIC:

Dark Web

Dark Net

Deep Web

Deep Net

Deep Dark

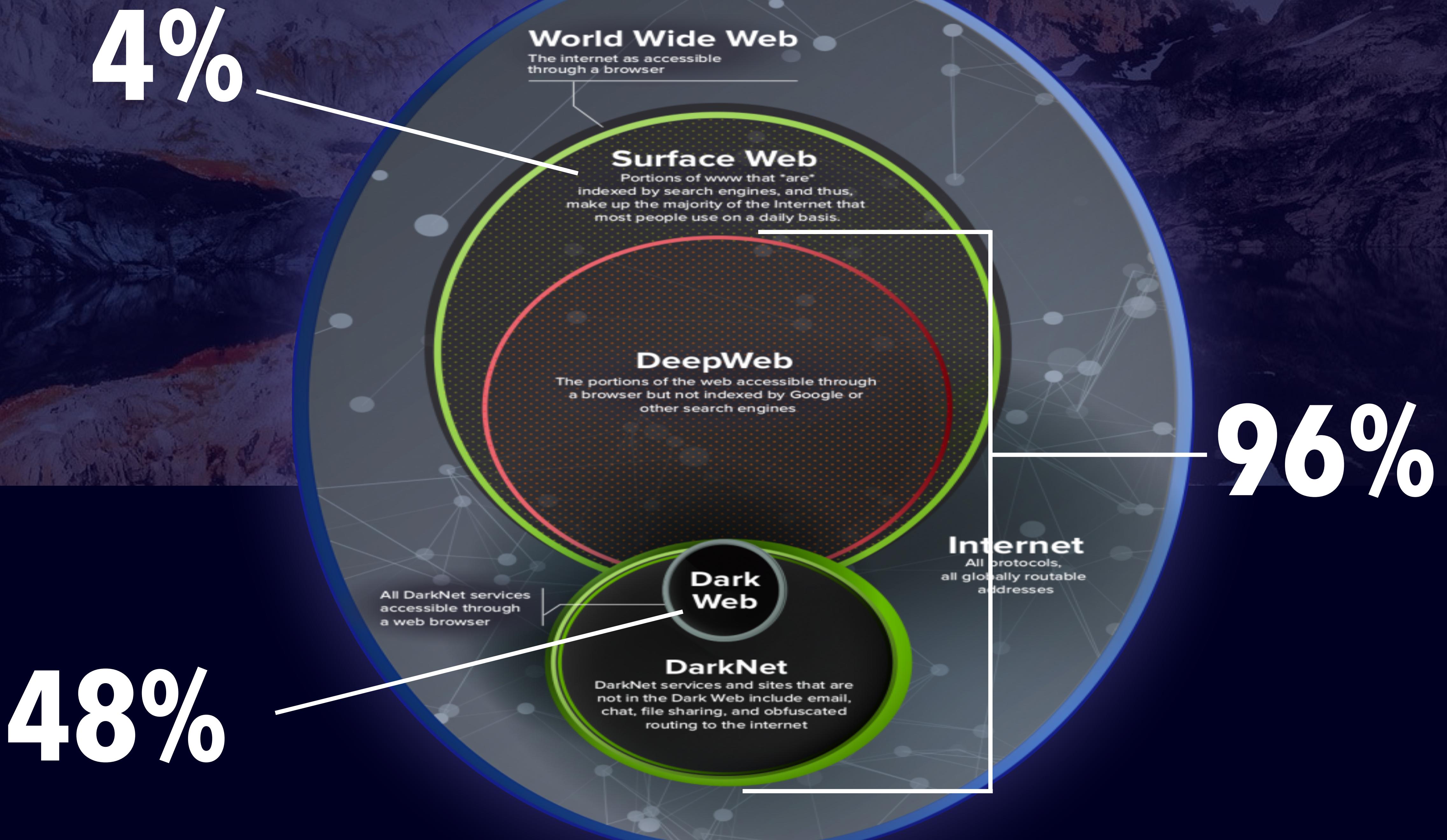
Dark Dark

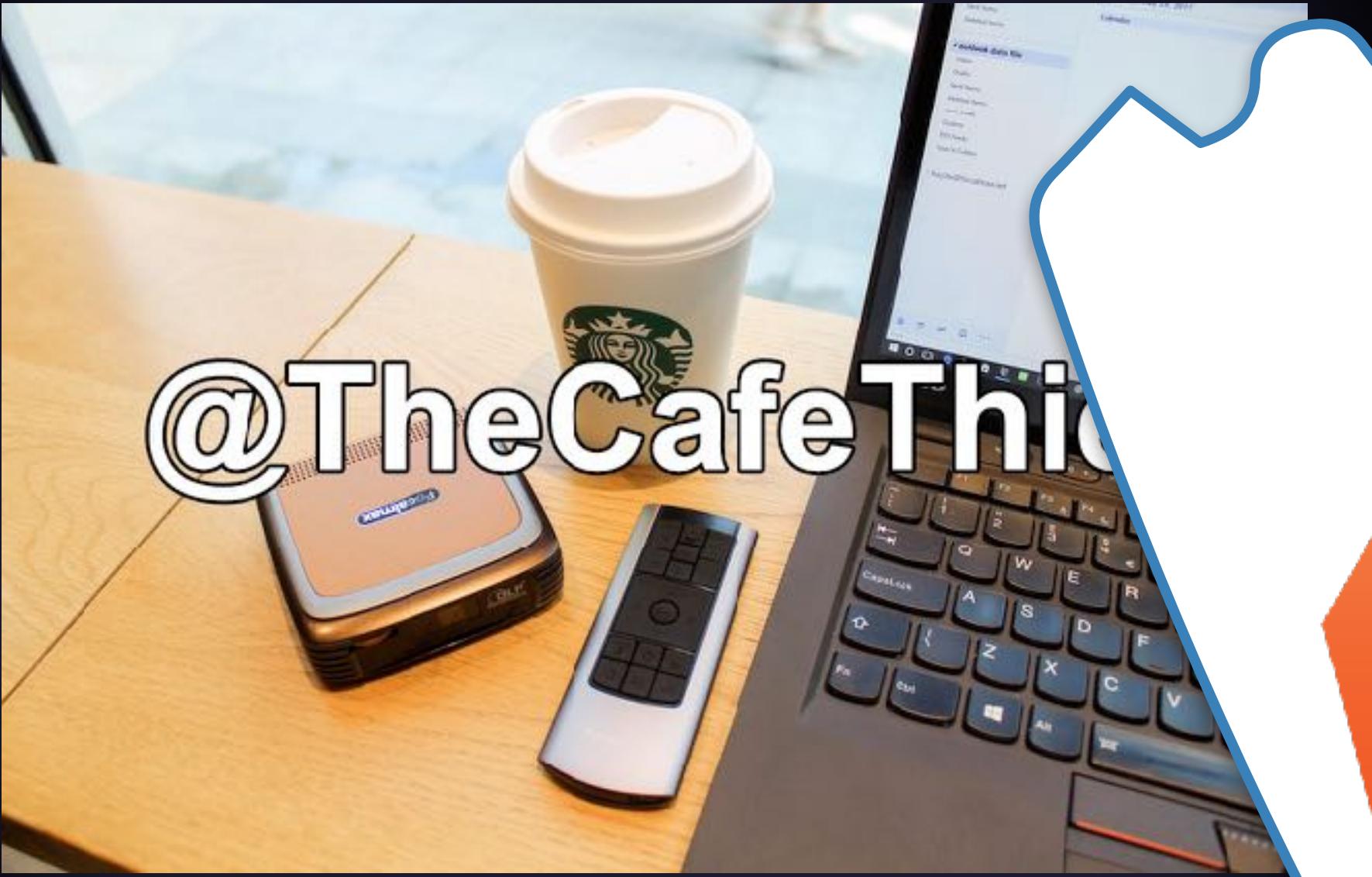
Dank Net

Derp Net

R'lyeh

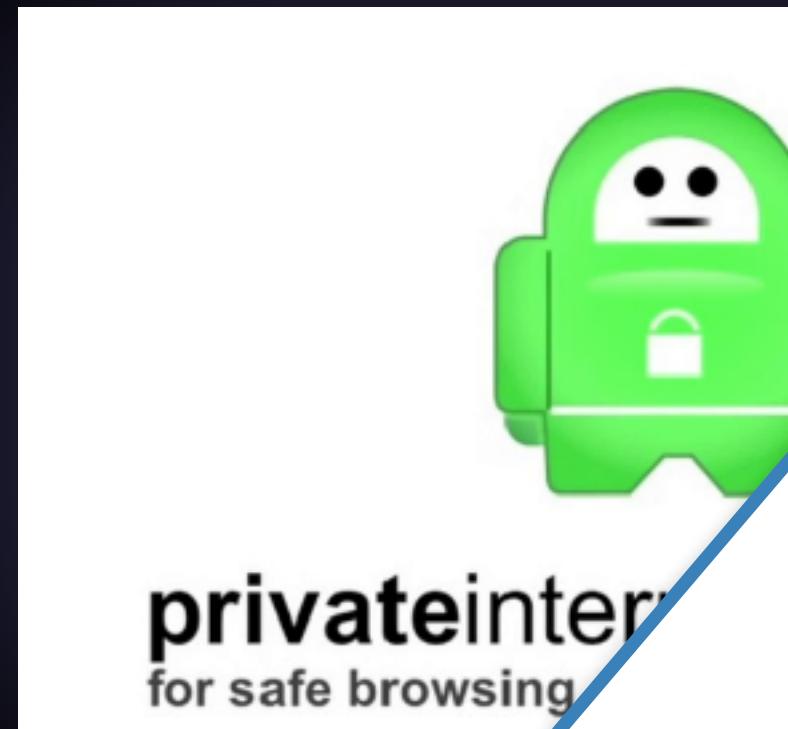
Beyond the Shire





@TheCafeThis

brave



```
[+] scanning (wlan0)
NUM ESSID
```

```
scanning intervals, CTRL+C will stop
-----
```

	POWER	WPS?	CLIENT	
1	A2	66db	wps client	
2	WPA	34db	no clients	
3	WPA2	27db	no client	
4	WPA	19db	wps clients	
5	2	WPA2	13db	no
6	WPA2	10db	wps client	
7	6	WPA2	10db	no

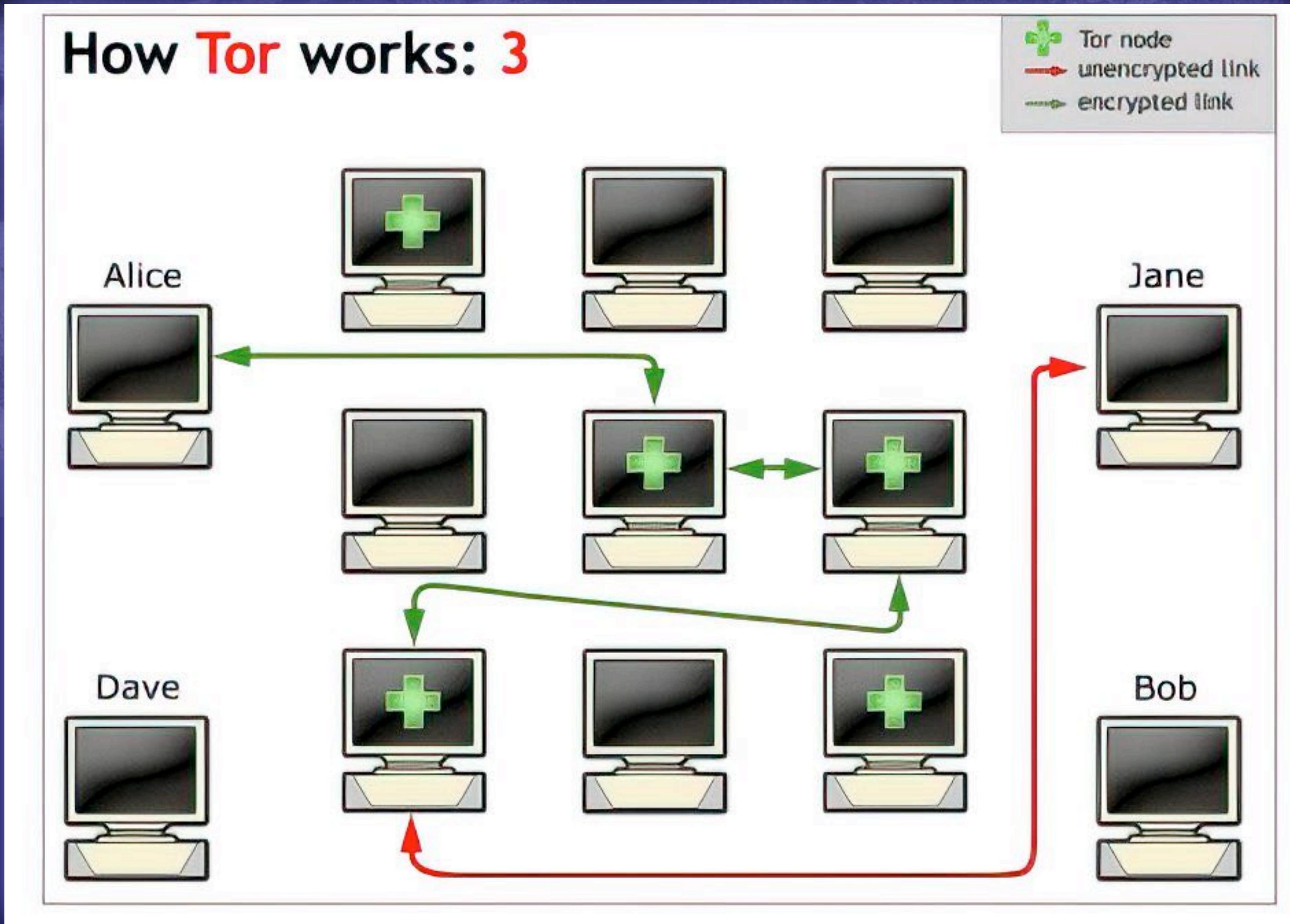
```
wireless networks. 7 targets and 10 clients found
```

- Military
- Political Activists / oppressed citizens
- Journalists
- Whistleblowers
- Cybercriminals \ Cybercrime Merchants



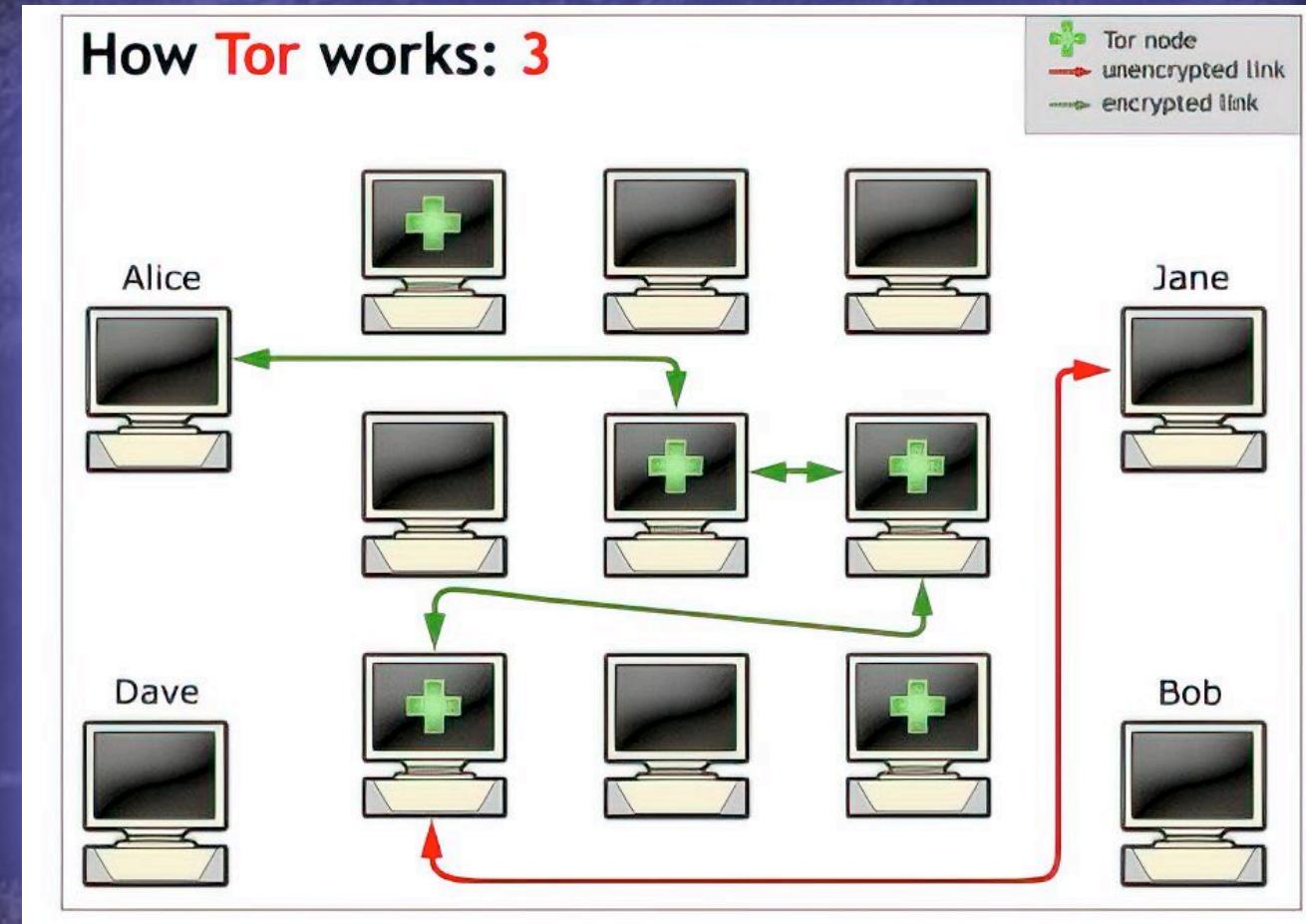
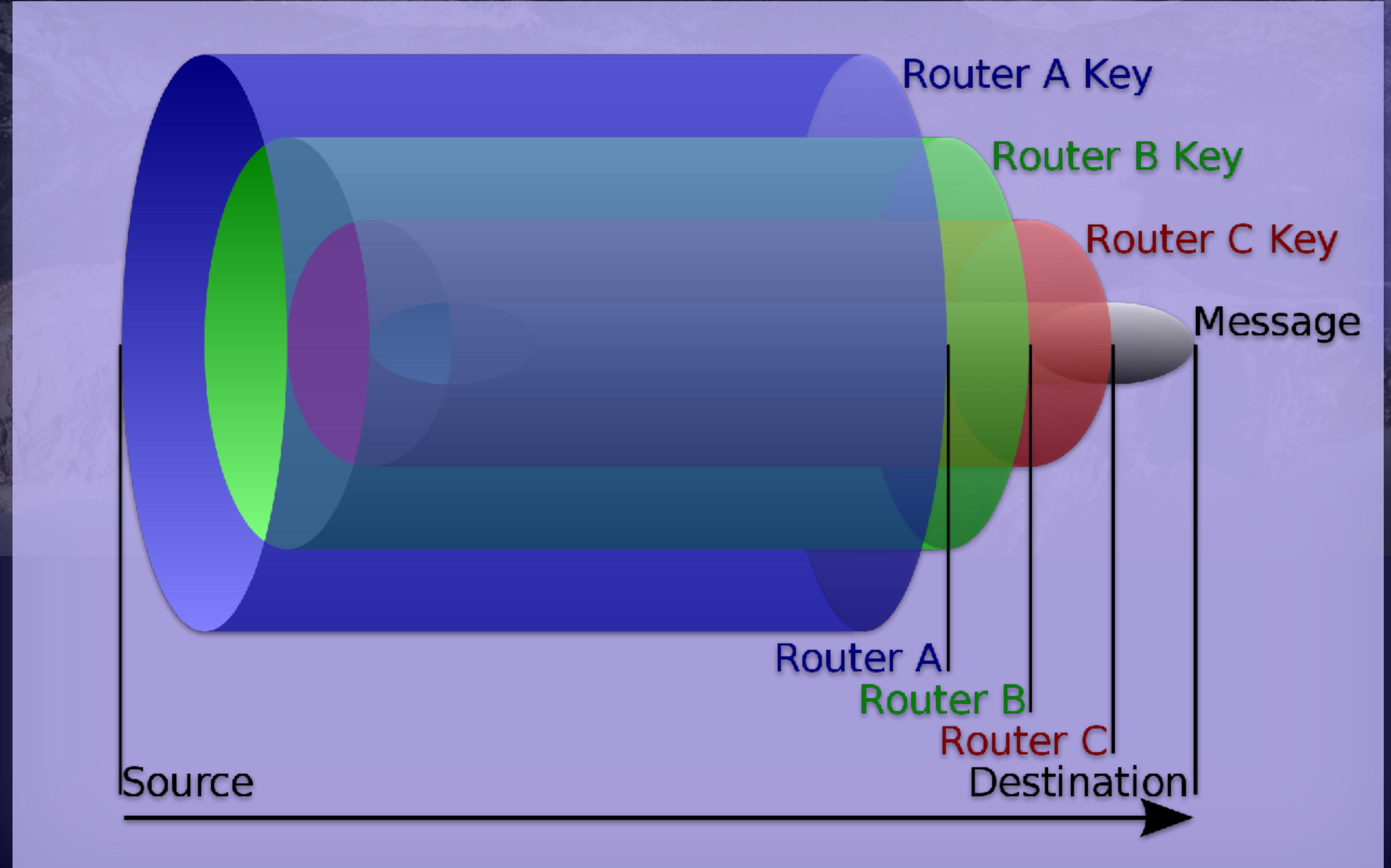
YES.

Tor Nodes \ "Routers":



Onion Routing:

Illuminating the Dark Web - SMFS, Inc. dba GRIMM



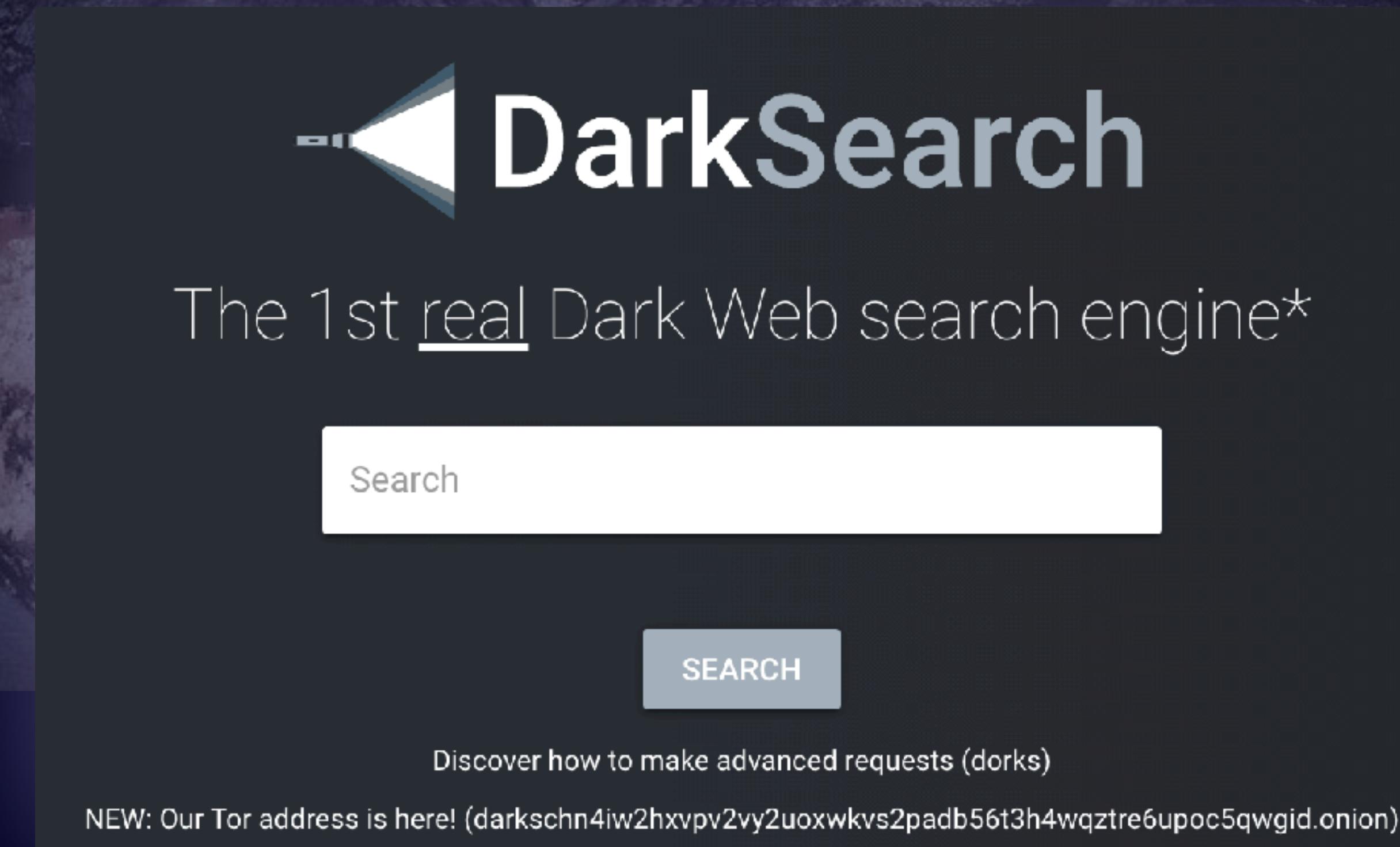


SURFING THE DARK WEB IS NOT ILLEGAL.

(in the US, at least)

Getting Started:

• Illuminating the Dark Web - SMFS, Inc. dba GRIMM



The screenshot shows the homepage of DarkSearch, a dark-themed search engine. At the top is a large logo consisting of a white megaphone icon followed by the word "DarkSearch" in a bold, white, sans-serif font. Below the logo is a subtext line: "The 1st real Dark Web search engine*". A large, light-gray rectangular input field contains the word "Search". Below this input field is a smaller, dark gray rectangular button with the word "SEARCH" in white capital letters. Underneath the search area is a link in a small, light-gray font: "Discover how to make advanced requests (dorks)". At the bottom of the page, there is a dark banner containing the text "NEW: Our Tor address is here! (darkschn4iw2hxvpv2vy2uoxwkvs2padb56t3h4wqztre6upoc5qwgid.onion)" in a light-gray font.

<https://www.deepwebsiteslinks.com/best-tor-sites/>

Legal Dark Web Activities:

- Facebook
- The New York Times
- The BBC
- Many EU Businesses
- Scandinavian Political Parties
- Personal Blogs
- SecureDrop, ZeroBin, ProtonMail
- Discussion Forums
 - Science, Technology, Gaming, Cooking,
 - Comic Books, Religion, Specific Diseases, etc.
 - Hidden Answers



CICADA 3301:

Illuminating the Dark Web - SMFS, Inc. dba GRIMM

Why Don't we all Hang Out Here?

- Often slow
- Unreliable search engines and results
- Entire communities disappear overnight
- Scams / malware galore
- High risk of seeing things you didn't want to
- Marketplaces are difficult to use and mostly scams



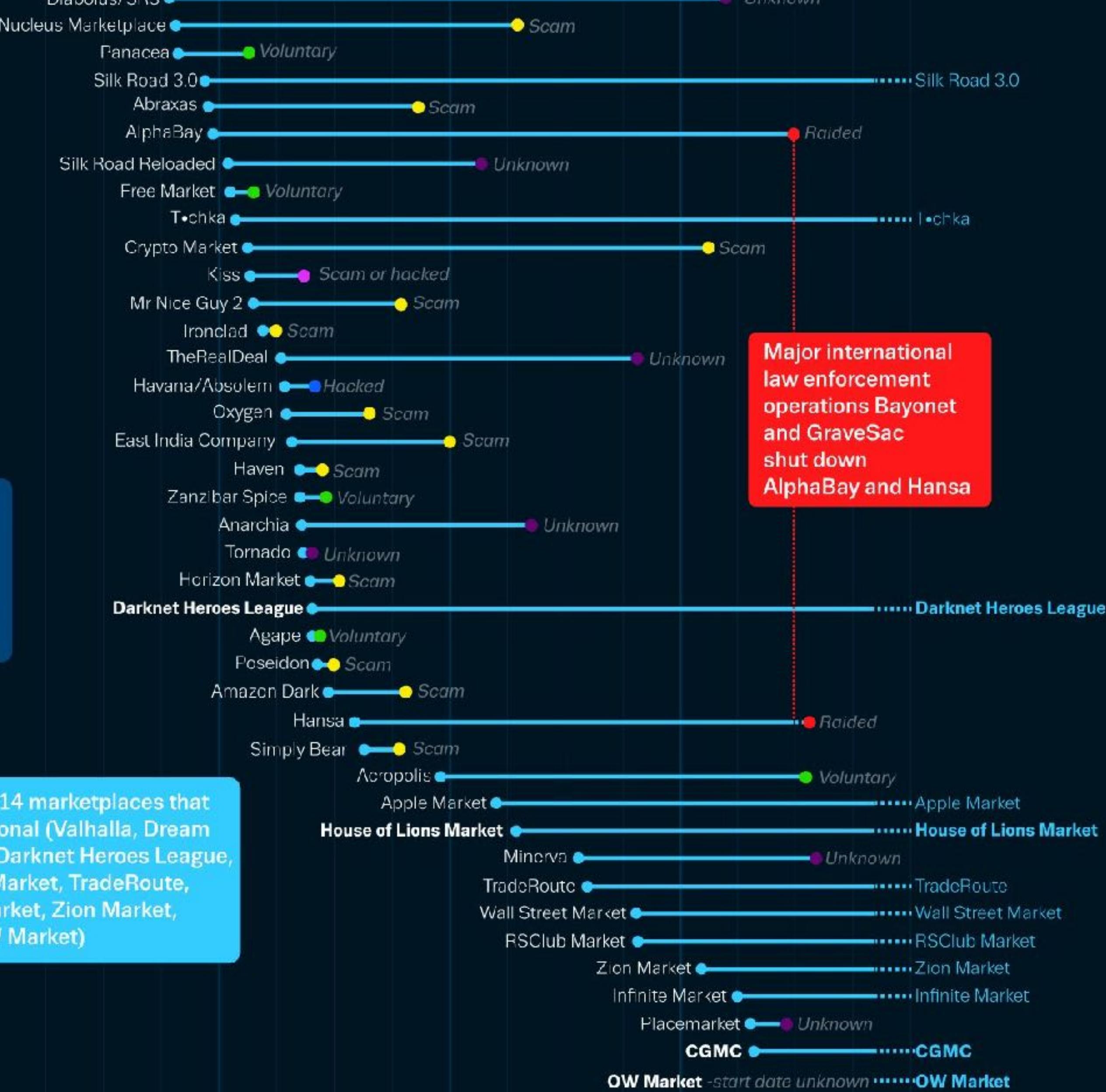
Illuminating the Dark Web - SMFS, Inc. dba GRIMM

Market status last checked on 28 June 2017
(except for AlphaBay and Hansa, for which data and information were updated to reflect closure on 28 June 2017 and 20 July 2017 respectively)

13 marketplaces (Hansa, Agora, Nucleus Marketplace, TheRealDeal, Acropolis, Middle Earth Marketplace, Apple Market, BlackBank Market, House of Lions Market, Evolution, Silk Road Reloaded, Silk Road 2.0 and Anarchia) – operated between one and two years

Nine marketplaces (Silk Road, AlphaBay, Silk Road 3.0, BlackMarket Reloaded, T•chka, Diabolus/SR3, The Farmer's Market, Darknet Heroes League and Crypto Market) have made it for a period of between two and three years

At the time of writing there are 14 marketplaces that appear to be active and operational (Valhalla, Dream Market, Silk Road 3.1, T•chka, Darknet Heroes League, Apple Market, House of Lions Market, TradeRoute, Wall Street Market, RSClub Market, Zion Market, Infinite Market, CGMC and OW Market)





SO WHAT CAN
WE BUY?

Marketplaces

- 67% of listings are for illegal physical contraband
- 17% are for Fraud / Counterfeiting (Mostly malware)
- “Empire” is the largest market currently
- Bitcoin, Litecoin & Monero are the common currencies
- Advances in online anonymity means more users
- Mystique has led to prices higher than the Clear Web.



Most common marketplace items:

Modafinil Tablets (Modalert) 10x200 MG



\$0.00195
Gfellas (440) (4.97★)
NL → EU

[Order](#)

NO ESCROW

25-ct Modafinil 200mg (Modvigil)



\$0.00713
themodsquad (540) (5.00★)
US → US

[Order](#)

NO ESCROW

Fluor-Modafinil 100g

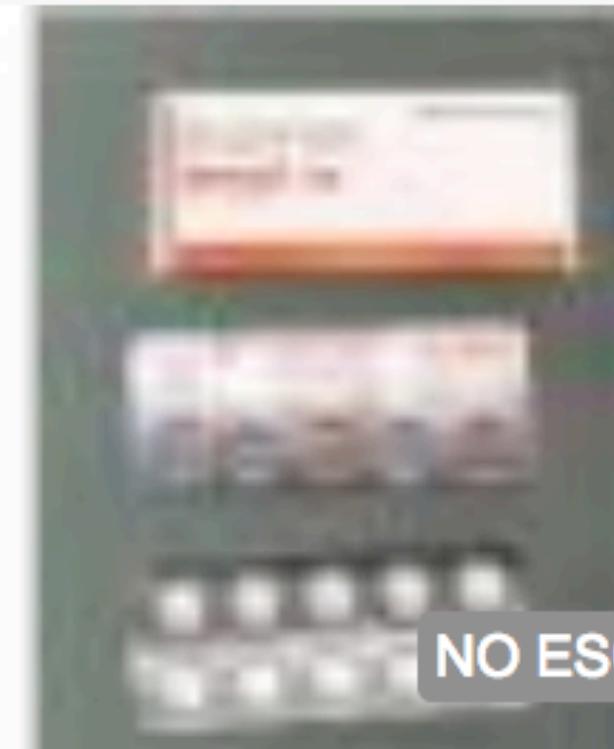


\$0.0716
ROCKETCHEM (270) (4.9★)
WW → WW, EU

[Order](#)

ESCROW

Nuvigil /Armodafinil 150mg - 300Pills



\$0.0423
indianpilldaddy1 (210) (4.76★)
IN → WW, AU

[Order](#)

NO ESCROW

Prescription-Only Medication

• Most common marketplace items:



■ [MS] [FE 50%] Nike Air Yeezy II Kanye West 40-46
1:1 Grade
Item # 213767 - Clothing / Clothing - RechardSport (632)

Views: 87 / Bids: Fixed price
Quantity left: Unlimited

Buy price
USD 450.00
(0.6184 BTC) 



■ [MS] White Chanel Classic Double Flap Lambskin Purse with Authenticity Card Retails for 3,500
Item # 151361 - Clothing / Clothing - stobyj (154)

Views: 1140 / Bids: Fixed price
Quantity left: Unlimited

Buy price
USD 325.00
(0.4466 BTC) 



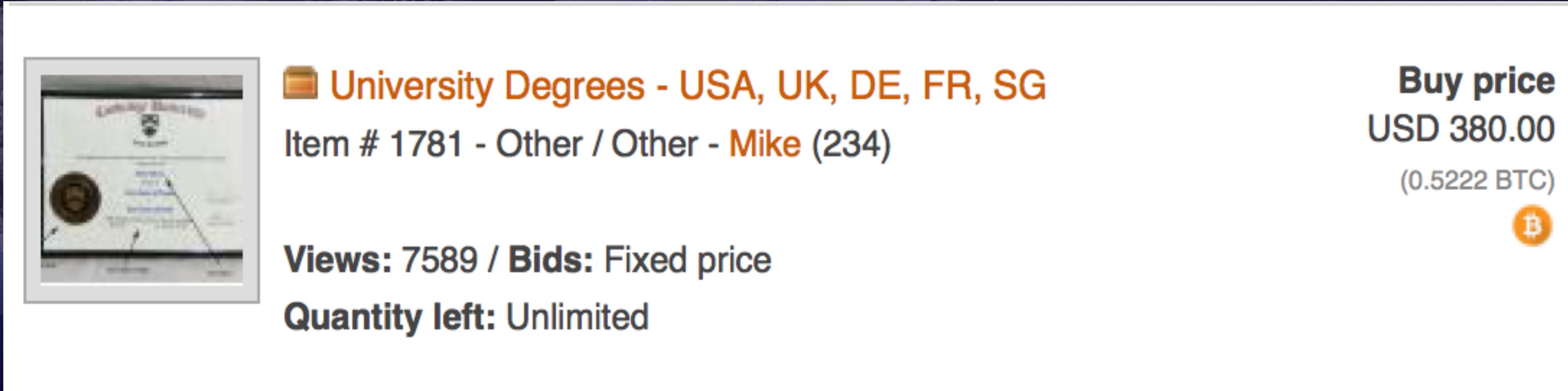
■ [MS] [FE 70%] Rolex - DATEJUST 18K Gold 36MM GWG [S-Factory] [AAA+]
Item # 47266 - Jewelry / Jewelry - sexyhomer (2608)

Views: 4861 / Bids: Fixed price
Quantity left: Unlimited

Buy price
USD 429.00
(0.5903 BTC) 

• Counterfeit Fashion

• Most common marketplace items:



University Degrees - USA, UK, DE, FR, SG

Item # 1781 - Other / Other - **Mike** (234)

Views: 7589 / Bids: Fixed price

Quantity left: Unlimited

Buy price
USD 380.00
(0.5222 BTC)



• VERIFIABLE Degrees from Accredited Schools

Most common marketplace items:



EU - Dutch Passport.
eufakes [+0|0] Level 1
Ships from: Europe (EU)

USD 3,332.77
฿ 4.5006
Buy Now
Views: 2825



Canada Profiles / Personnal data (No cc)

Canadian Profile including : First Name, Middle, Last Name
DOB Full Address Phone number Email (NO password)
SIN/SSN Name of Employer Salary (Not for all, +- 7/10) DL
(If applicable) MMN is NOT included, sorry guys
Lastname:Middlename:Firstname:DOB(YYMMDD):Address:To
auto-fulfill ONLY applicable for random listing Postage
options ...

Sold by REDFOX - 615 sold since Aug 20, 2015 **Vendor**
Level 5 **Trust Level 6**
81 items available for auto-dispatch

Passports \ Entire New Identities

Most common marketplace items:

1 lb Pure Sand



Seller GarageSale [515 - 53] **Price** USD 5.71
฿ 0.0128 **Quantity** 18 in stock **Currency** USD **Shipping options** Europe [3 days] [+ USD 14.85]

Description

Like from the n _____ beach, yo! Guaranteed pure with no additional cuts or adulterants (Screw those random bottle caps and cigarette butts! Nobody needs that _____). Get your pound of sand today and be the envy (and possibly the laughing stock) of all your friends.

Pet Brick

USD 5.71
฿ 0.0128 **18 in stock**

Shipping options Europe [3 days] [+ USD 14.85]

Vendor	FlaminSpy [+0 0]	Level 1 (0)
Class	Physical	
Ships From	Netherlands	
Ships To	Europe (EU)	

"Other"

Most common marketplace items:

dubrovački vjesnik

A NEW TWIST IN THE INVESTIGATION OF TRANSPORT RADIO OVER 226 CROATIAN

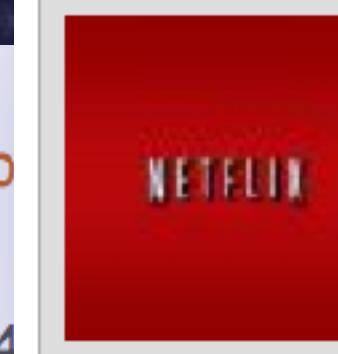
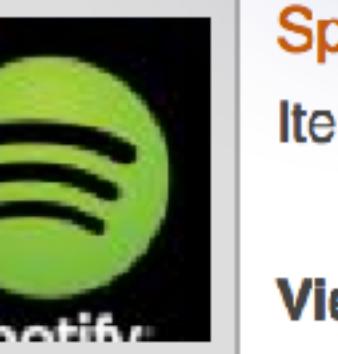
The Pole now says: radium 226 I took in Poland for an alternative treatment!

R-226 has been documented to be 2.7 million times more radioactive than its molar weight in natural uranium. Exposure has caused innumerable deaths.

statement; the home contained proof of similar darknet purchases. Many pieces of jewelry contained radioactive substances, investigators said. The

Uranium

Most common marketplace items:

	<p>[Bulk] Xfinity Premium Account + Wifi Ho [LIFETIME + FREEBIES] Item # 8602 - Other / Other - DrawkwarD (94010)</p> <p>Views: 21838 / Bids: Fixed price Quantity left: Unlimited</p>		<p>[MS] 100 Netflix Accounts [LIFETIME + FREEBIES] Item # 89668 - Other / Other - DrawkwarD (94010)</p> <p>Views: 3110 / Bids: Fixed price Quantity left: Unlimited</p>	<p>Buy price USD 9.99 (0.0135 BTC)</p> 
	<p>UFC Fight Pass [LIFETIME + FREEBIES] Item # 8955 - Other / Other - DrawkwarD (94009)</p> <p>Views: 5046 / Bids: Fixed price Quantity left: Unlimited</p>		<p>Item # 8603 - Other / Other - Drawkward (94009)</p> <p>Views: 10031 / Bids: Fixed price Quantity left: Unlimited (8 automatic items)</p>	<p>Buy price USD 0.99</p> 
	<p>[MS] US Uber Account [LIFETIME + FREEBIES] Item # 120893 - Other / Other - DrawkwarD (94009)</p> <p>Views: 15786 / Bids: Fixed price Quantity left: Unlimited</p>		<p>Spotify Premium Account [LIFETIME + FREEBIES] Item # 8599 - Other / Other - DrawkwarD (94009)</p> <p>Views: 101982 / Bids: Fixed price Quantity left: Unlimited (24 automatic items)</p>	<p>Buy price USD 1.95 (0.0026 BTC)</p> 
			<p>(0.0067 BTC)</p> 	

Guaranteed Lifetime Accounts

Most common marketplace items:



Xls Silent FUD Exploit 3 Copies
Item # 231190 - Exploits / Exploits - **Exploit (0)**

Views: 54 / Bids: Fixed price
Quantity left: 3



0Day Exploit | Silent AV |
Item # 227645 - Exploits / Exploits - **Exploit (0)**

Views: 94 / Bids: Fixed price
Quantity left: 3

EAT SUBWAY FOR FREE - exploit method

Vendor g3cko (2850) (4.79★) (a 44/3/4) (o 346/5/5)
Price \$0.0002908 (\$2.0696)
Ships to Worldwide
Ships from Worldwide
Escrow Yes



0-Days & Exploits

• Most common marketplace items:

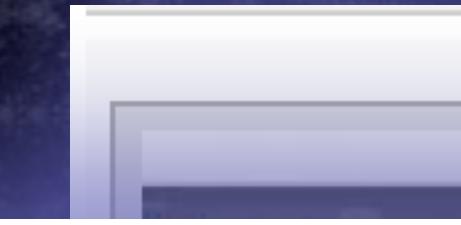


[MS] XKey Private Keylogger

Item # 52351 - Botnets & Malware / Botnets & Malware -
ja_far (1)

Views: 207 / Bids: Fixed price

Quantity left: Unlimited



[MS] CyberGate_v3.4.2.2 Full Private RAT

Item # 29447 - Botnets & Malware / Botnets & Malware -

Buy price USD 50.00

(0.0691 BTC)

28 / Bids: Fixed price

Quantity left: Unlimited (1 automatic items)

Buy price

USD 5.51

(0.0076 BTC)



DROID JACK Andriod RAT

Item # 19227 - Botnets & Malware / Botnets & Malware -
shonajaan (12155)

Buy price

USD 2.20

(0.0030 BTC)



GovRAT [Soruce Code + 1 Code Signing Cert Included]

Item # 8348 - Botnets & Malware / Botnets & Malware -
bestbuy (439)

Views: 1692 / Bids: Fixed price

Quantity left: Unlimited

Buy price
USD 2,000.00

(2.7640 BTC)



Password Stealers & Backdoor Apps

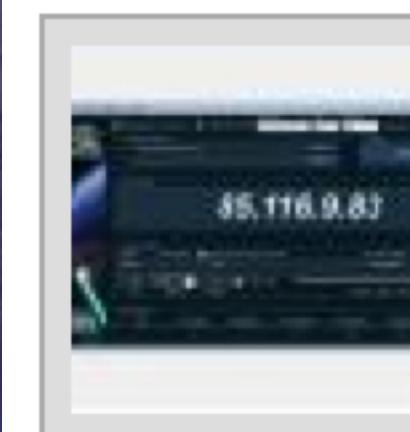
• Most common marketplace items:



Zeus Botnet
Item # 8305 - Botnets & Malware / Botnets & Malware - shonajaan (12155)

Views: 15296 / **Bids:** Fixed price
Quantity left: Unlimited (2453 automatic items)

Buy price
USD 3.30
(0.0046 BTC)
฿



[MS] ★LOIC - DDOS attack tool★
Item # 61760 - Botnets & Malware / Botnets & Malware - magrin (117)

Views: 221 / **Bids:** Fixed price
Quantity left: Unlimited

Buy price
USD 3.00
(0.0041 BTC)
฿



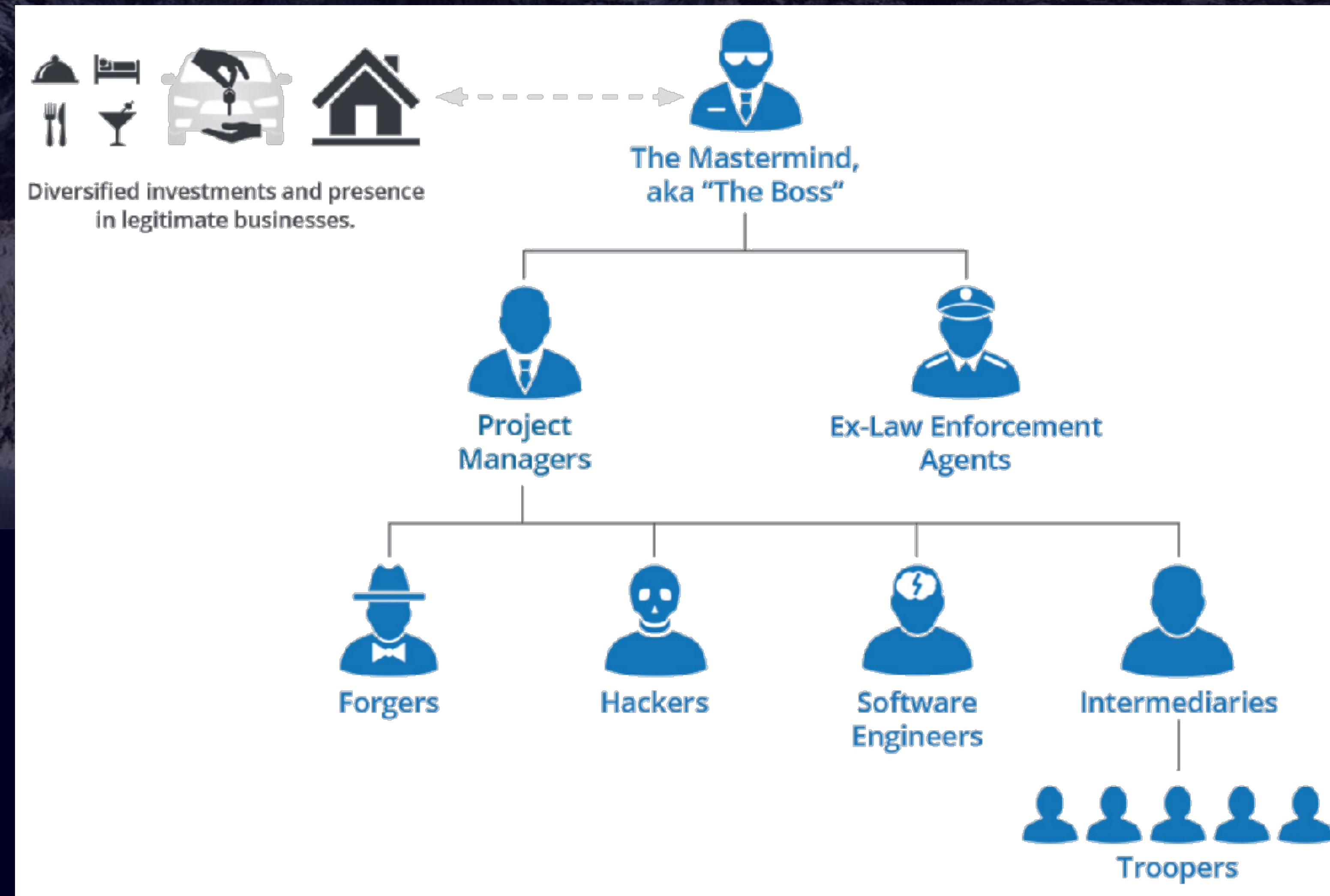
[MS] ~ Atmos Banking Trojan Builder + Canada...
Webinjects ~
Item # 150711 - Botnets & Malware / Botnets & Malware - mastercorp (2308)

Views: 1709 / **Bids:** Fixed price
Quantity left: Unlimited (17 automatic items)

USD 25.00
(0.0346 BTC)
฿

• Botnet & Ransomware Source Code (& Scams)

A note on malicious software



Also: Ransomware as a Service!

Most common marketplace items:

Pages (2): 1 2 Next » Thread Rating: ★★★★★

Need a hacker? n0rf@sigaint.org Thread Modes

! 08-13-2016, 05:10 PM (This post was last modified: 09-24-2016, 06:40 PM by n0rf.) #1



n0rf • Vocal Member ★★★

Posts: 221, Threads: 71 Joined: Aug 2016 Reputation: 2

Hello! I am n0rf and have been programming and hacking for about 7 years. I am very active in the hacking community and would love to help or partner with you.

I offer many different services for extremely low prices. If you want to contact me email me at n0rf@sigaint.org!

Hacking-as-a-Service

Most common marketplace items:

Scammer Report - Unresolved

Scammed by MakingEZMoneyForYou

Discussion in 'Scam Reports' started by FacelessSoldier, Oct 5, 2016.

Scammer Report - Unresolved

christ123 - Beware

Discussion in 'Scam Reports' started by ShardzRus, Mar 10, 2016.

Scammer Report - Unresolved

Scammed by FraudResource for 2000\$ GRAND SCAM

Discussion in 'Scam Reports' started by babagana, Oct 1, 2016.

Scammer Report - Unresolved

DISCOUNT DEPOT IS A SCAM

Discussion in 'Scam Reports' started by martian727, Sep 7, 2016.

Scammer Report - Unresolved

Buy at your own risk from FastandSafe

Discussion in 'Scam Reports' started by ghost1960, Sep 16, 2016.

Scammer Report - Unresolved

i was scammed by EscrowEscobar

Discussion in 'Scam Reports' started by opiatepope, Oct 3, 2016.

Scams, Scams, Scams

Most common marketplace items:



FEDS, FEDS, FEDS

•
•
•
THANK YOU / Q & A

JOHNNY XMAS

SENIOR SECURITY RESEARCHER
&
SENIOR TRAINER

SMFS, INC. (GRIMM)

[HTTPS://GRIMM.RIP](https://GRIMM.RIP)



[HTTPS://GRIMM.RIP](https://GRIMM.RIP)

DECKS AT: LINKTR.EE/JOHNNYXMAS