ISS News

Vladimír Veselý
2019-09-09

Agenda

- OSINT
- TOR

Anders Brejvik

Anders Behring Breivik

Sketch of Breivik

Born	13 February 1979 (age 40) Oslo, Norway
Status	Imprisoned
Nationality	Norwegian
Height	6 ft (183 cm)
Weight	176 lb (80 kg)

2011 Norway attacks

31 minutes after the explosion in Oslo

Locations of the incidents in the Oslo and Buskerud counties of Norway

Location	Oslo and Utøya, Norway
Coordinates	59°54′54″N 10°44′48″E
Date	22 July 2011 **Oslo:** 15:25[1] CEST **Utøya:** 17:22–18:34 CEST[2][3] (UTC+02:00)
Target	Labour Party[4][5]
Attack type	Car bomb, mass shooting, terrorism
Weapons	**Oslo:** Car bomb (made using ANFO) **Utøya:** Semi-automatic rifle (Ruger Mini-14) and semi-automatic pistol (Glock 34)[6]
Deaths	**Oslo:** 8 **Utøya:** 69 (67 from gunfire) **Total: 77**[7][8]
Injuries	**Oslo:** At least 209 **Utøya:** At least 110 (32 by gunfire)[9] **Total: At least 319**[10][11][12]
Perpetrator	Anders Behring Breivik
Motive	Far-right extremism, Islamophobia[13]

Anders Brejvik

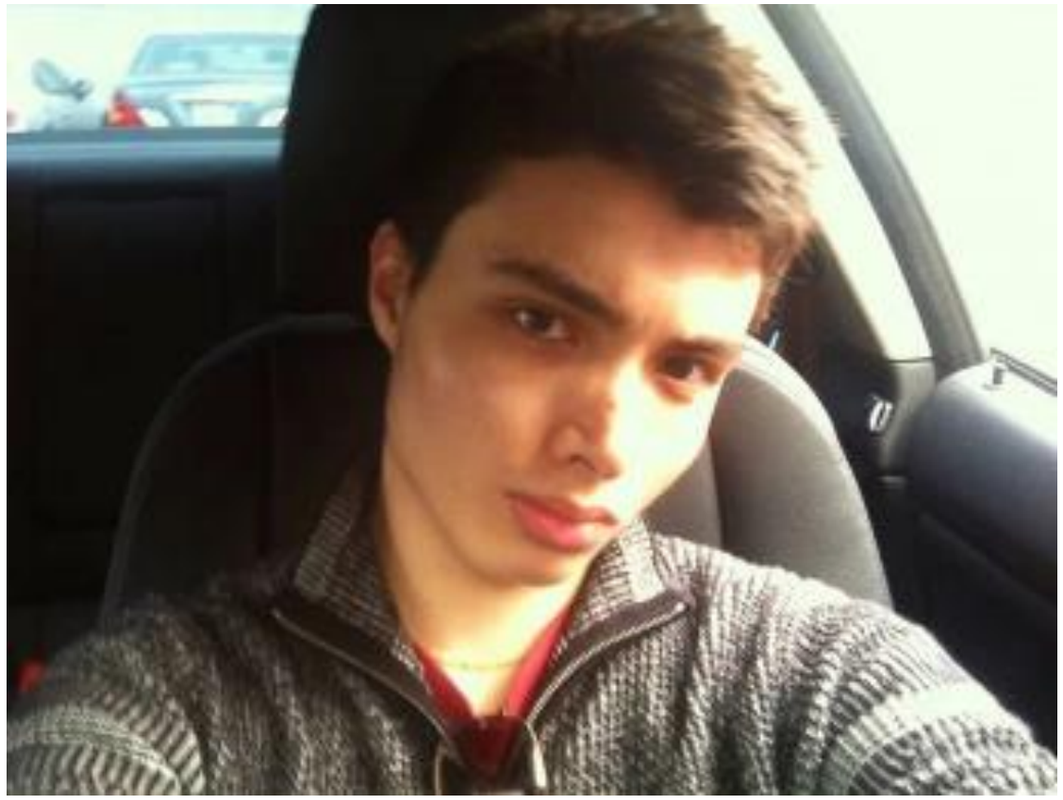
- Joined 2009 on a forum on mass murdering, killing sprees, he talked about his admiration to mass murders

- Playing School Shooter game (HL2 mod)
- He did tactical reloading in the act (inspiration from games)

- He was posting violent photographs/videos on 4chan
- On 4chan he also posted about the fact he was going to die tomorrow

Elliot Rodger

- *"I didn't start this war... I wasn't the one who struck first... But I will finish it by striking back. I will punish everyone. And it will be beautiful. Finally, at long last, I can show the world my true worth."*



2014 Isla Vista killings

Isla Vista (southern California)

Location	Isla Vista, California, United States
Coordinates	34.412°N 119.859°W
Date	May 23, 2014 ~9:27 p.m. (UTC−8:00)
Target	Students of the University of California, Santa Barbara
Attack type	Spree killing · murder–suicide · drive-by shooting · stabbing · vehicle-ramming attack
Weapons	Two knives · Glock 34 handgun · Two SIG Sauer P226 handguns · BMW 328i Coupé
Deaths	7 (3 by stabbing, 4 by gunfire including the perpetrator)
Injuries	14 (7 by gunfire, 7 struck by motor vehicle)
Perpetrator	Elliot Rodger
Motive	Revenge for perceived sexual and social rejection

Elliot Rodger

- On April 30, Rodger's parents saw his YouTube videos and became alarmed by them, so they contacted police. However, when the officers interviewed Rodger at his apartment, he downplayed the situation. They decided "he did not meet the criteria for an involuntary [mental health] hold", nor was there any reason to legally search his residence, so they left.

- Rodger's final YouTube video was discovered after the killing spree by parents 2 days later and deleted from the website.

- However, it was already too late, for it had been copied and re-posted by other users beforehand.

Ismaaiyl Abdullah Brinsley

2014 killings of New York City Police Department officers

- ◉ Show map of New York City
- ○ Show map of New York
- ○ Show map of the United States
- ○ Show all

Location	Bedford–Stuyvesant, Brooklyn, New York City, New York, U.S.
Coordinates	40.695886°N 73.946494°W
Date	December 20, 2014; 4 years ago 2:47 p.m. (EST)
Attack type	Murder–suicide
Weapons	Taurus PT92 handgun
Deaths	3 (including the perpetrator)
Victims	2 (NYPD officers Rafael Ramos and Wenjian Liu)
Perpetrator	Ismaaiyl Abdullah Brinsley
Motive	Revenge for Eric Garner's and Michael Brown's deaths

Ismaaiyl Abdullah Brinsley

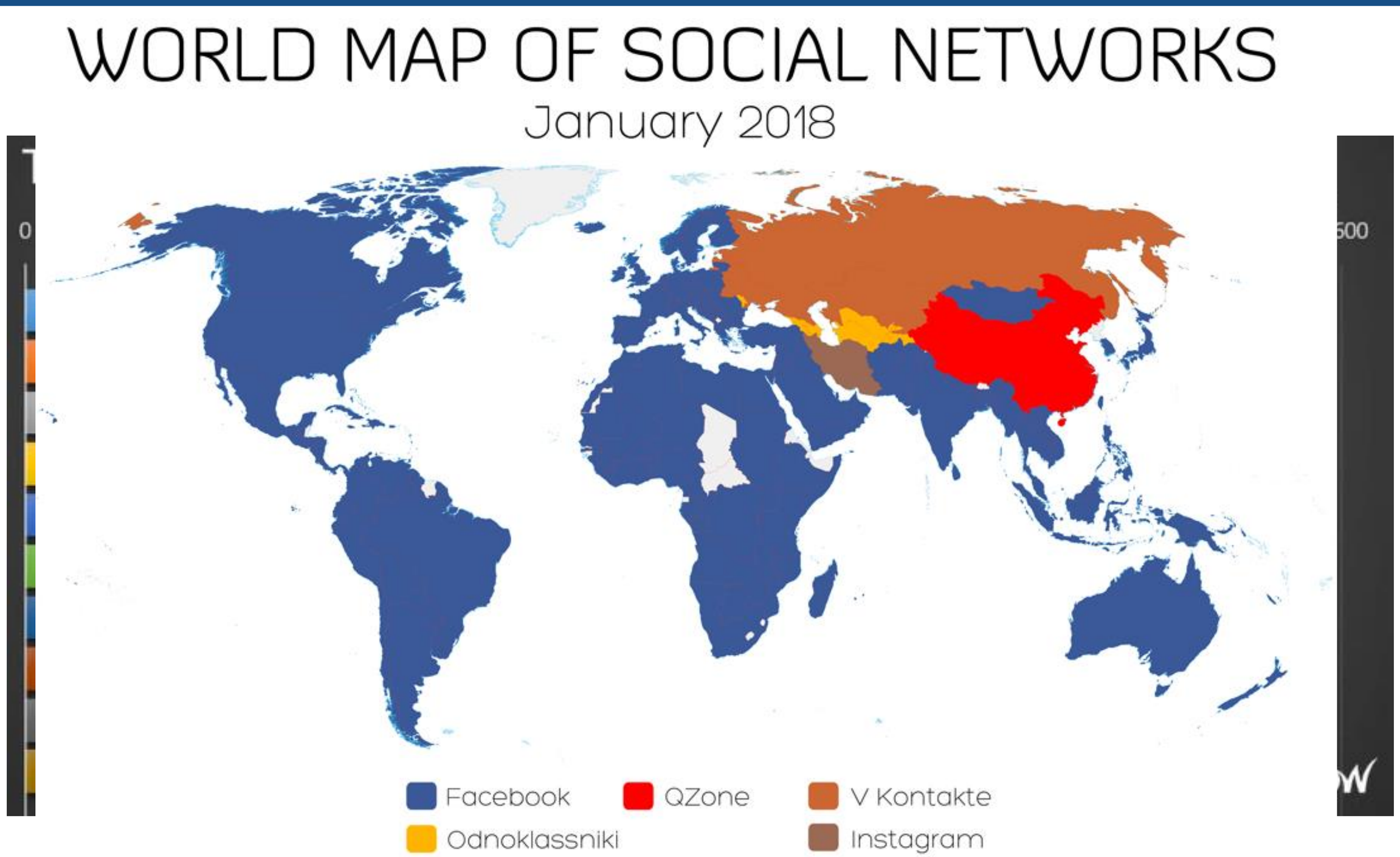
- Facebook profile - Blue Baracude, Instagram - same image - Gmail account – YT channel

- Posted his intentions on FB

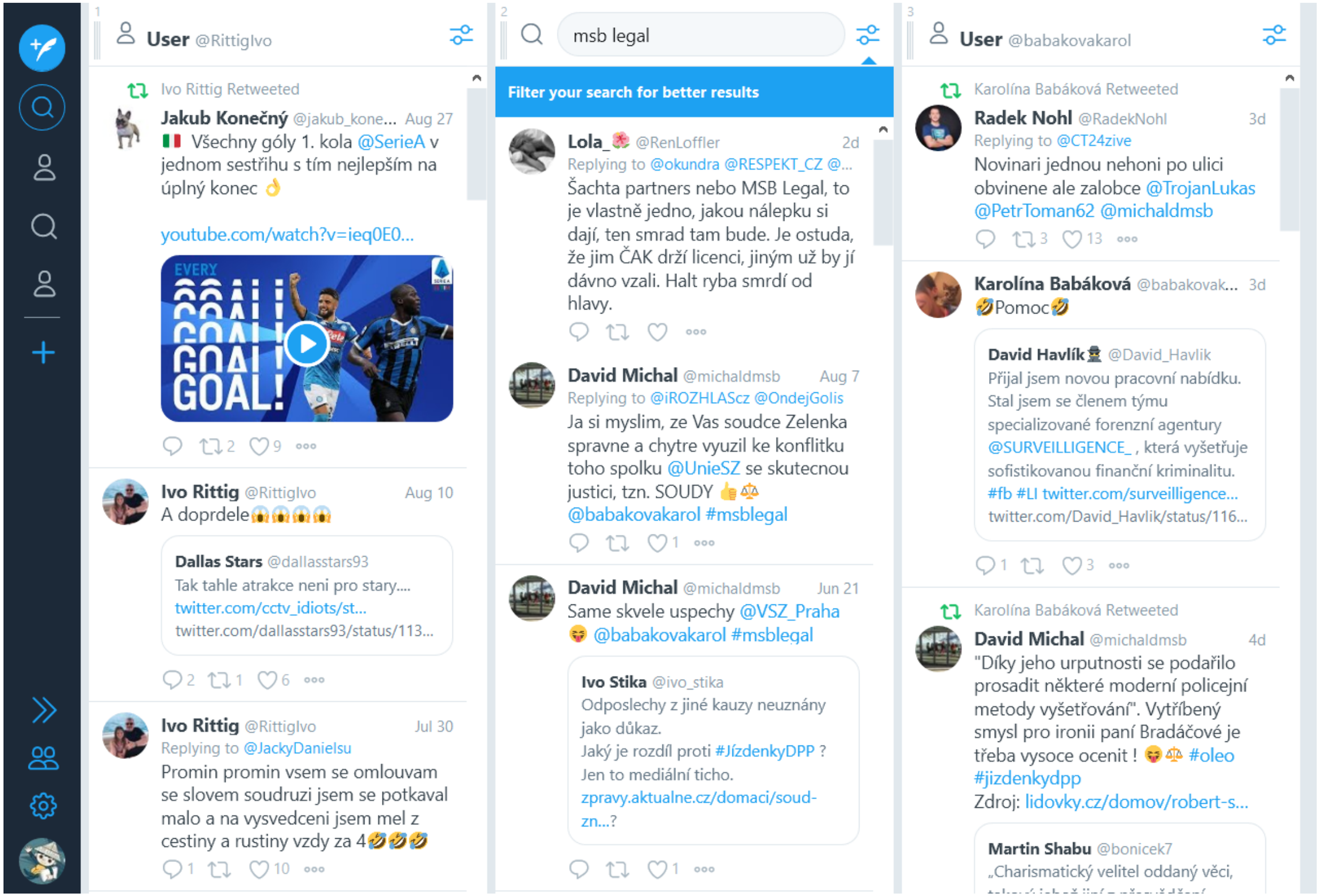
- Tried to find police officers FB and on Waze (where he communicated with other users in the search for police)

- Officer's son posting the fact his father died on Facebook the same day

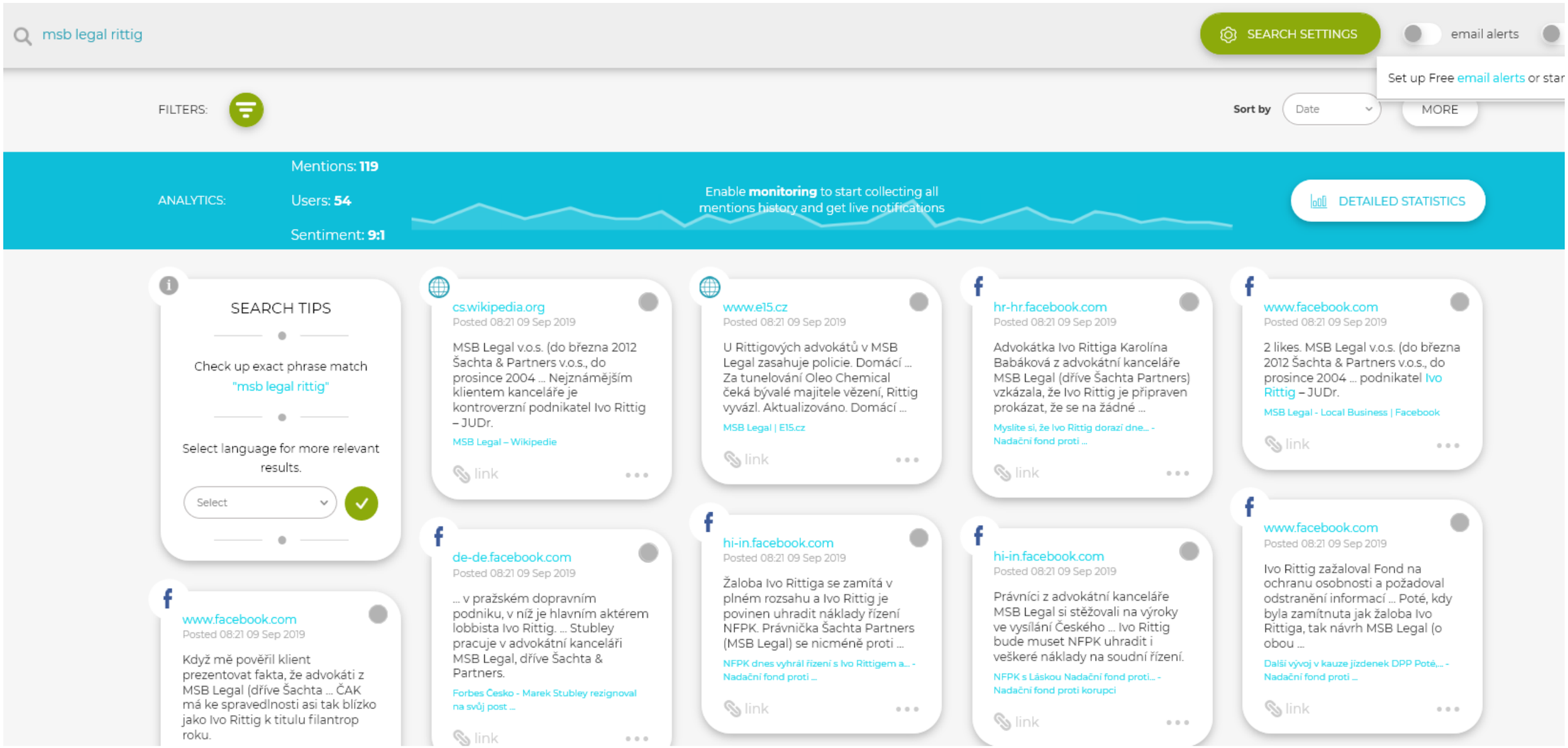
Ecosystem


WORLD MAP OF SOCIAL NETWORKS
January 2018
0
500
Facebook
QZone
V Kontakte
Odnoklassniki
Instagram
credits: Vincenzo Cosenza vincos.it
license: CC-BY-NC
source: Alexa/SimilarWeb

Tweet Deck


1
User @RittigIvo
Ivo Rittig Retweeted
Jakub Konečný @jakub_kone... Aug 27
🇮🇹 Všechny góly 1. kola @SerieA v jednom sestřihu s tím nejlepším na úplný konec 👌
youtube.com/watch?v=ieq0E0...
EVERY GOAL! GOAL! GOAL!
2 9
Ivo Rittig @RittigIvo Aug 10
A doprdele😱😱😱😱
Dallas Stars @dallasstars93
Tak tahle atrakce neni pro stary....
twitter.com/cctv_idiots/st...
twitter.com/dallasstars93/status/113...
2 1 6
Ivo Rittig @RittigIvo Jul 30
Replying to @JackyDanielsu
Promin promin vsem se omlouvam se slovem soudruzi jsem se potkaval malo a na vysvedceni jsem mel z cestiny a rustiny vzdy za 4🤣🤣🤣
1 10
2
msb legal
Filter your search for better results
Lola_🌺 @RenLoffler 2d
Replying to @okundra @RESPEKT_CZ @...
Šachta partners nebo MSB Legal, to je vlastně jedno, jakou nálepku si dají, ten smrad tam bude. Je ostuda, že jim ČAK drží licenci, jiným už by jí dávno vzali. Halt ryba smrdí od hlavy.
David Michal @michaldmsb Aug 7
Replying to @iROZHLAScz @OndejGolis
Ja si myslim, ze Vas soudce Zelenka spravne a chytre vyuzil ke konflitku toho spolku @UnieSZ se skutecnou justici, tzn. SOUDY 👍⚖️ @babakovakarol #msblegal
1
David Michal @michaldmsb Jun 21
Same skvele uspechy @VSZ_Praha 😜 @babakovakarol #msblegal
Ivo Stika @ivo_stika
Odposlechy z jiné kauzy neuznány jako důkaz.
Jaký je rozdíl proti #JízdenkyDPP ?
Jen to mediální ticho.
zpravy.aktualne.cz/domaci/soud-zn...?
1
3
User @babakovakarol
Karolína Babáková Retweeted
Radek Nohl @RadekNohl 3d
Replying to @CT24zive
Novinari jednou nehoni po ulici obvinene ale zalobce @TrojanLukas @PetrToman62 @michaldmsb
3 13
Karolína Babáková @babakovak... 3d
🤣Pomoc🤣
David Havlík🕵 @David_Havlik
Přijal jsem novou pracovní nabídku. Stal jsem se členem týmu specializované forenzní agentury @SURVEILLIGENCE_ , která vyšetřuje sofistikovanou finanční kriminalitu. #fb #LI twitter.com/surveilligence...
twitter.com/David_Havlik/status/116...
1 3
Karolína Babáková Retweeted
David Michal @michaldmsb 4d
"Díky jeho urputnosti se podařilo prosadit některé moderní policejní metody vyšetřování". Vytříbený smysl pro ironii paní Bradáčové je třeba vysoce ocenit ! 😜⚖️ #oleo #jizdenkydpp
Zdroj: lidovky.cz/domov/robert-s...
Martin Shabu @bonicek7
„Charismatický velitel oddaný věci,

Social Searcher



BuzzSumo

BuzzSumo | Content Research | Influencers | Monitoring | Try BuzzSumo Pro | Projects | Login

Topic Explorer New! | Content Analyzer | Facebook Analyzer | Question Analyzer | Trending Now | Backlinks

Content Analyzer

Search | Analysis

Ivo Rittig — Search — Save Search — Export — Total Results: 15

How to run an Advanced Search

Filter by Date
- 24 Hours
- Past Week
- Past Month
- Past 6 Months
- Past Year
- Past 2 Years
- Past 5 Years
- Specific Range

Only B2B Publishers

Country (TLD)

Language

Filter Domains

Content Type

Word Count

Publisher Size

Apply Filters

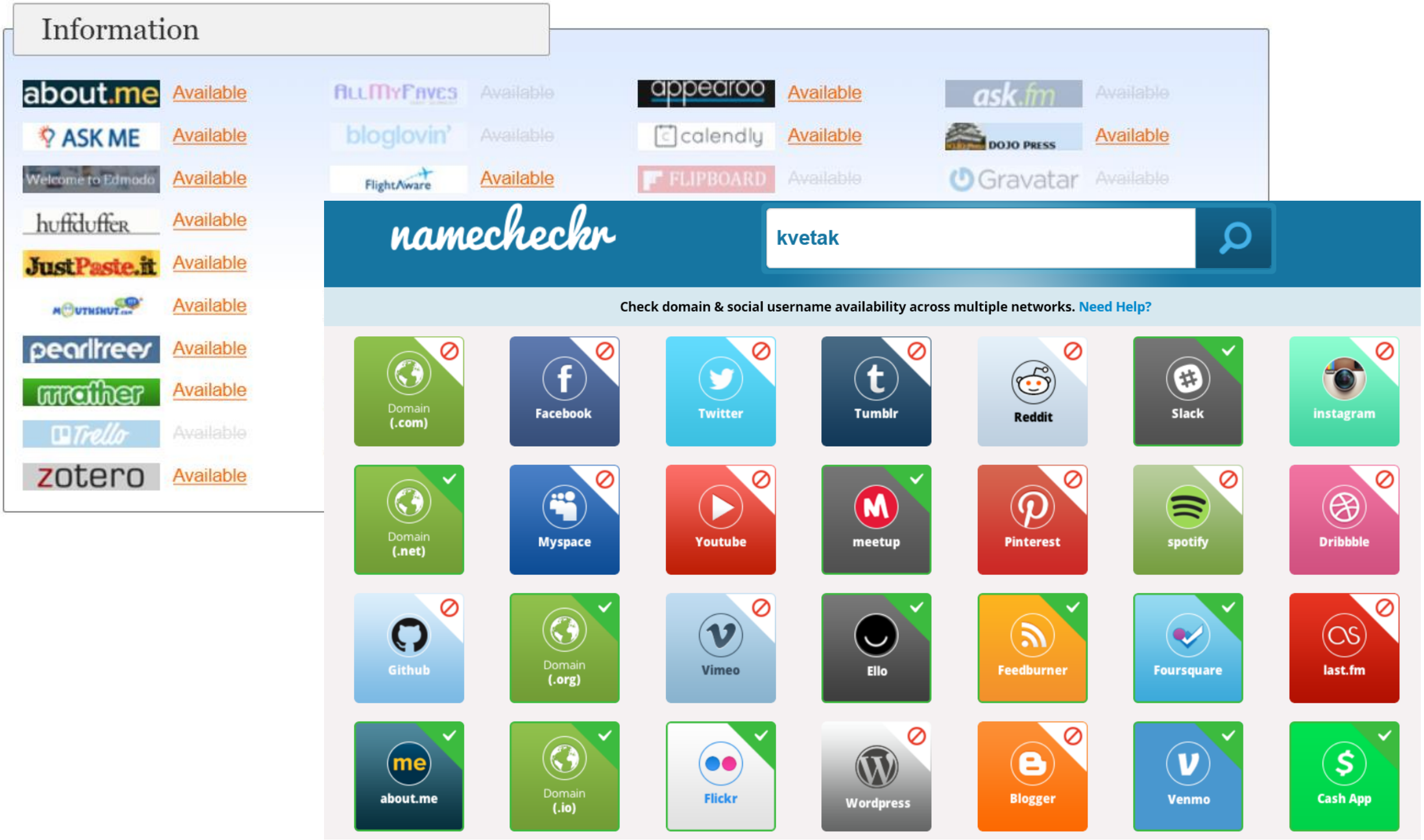
Reset Filters

Sort by: Total Engagements

		Facebook Engagements	Twitter Shares	Pinterest Shares	Reddit Engagements	Number of Links	Evergreen Score	Total Engagements
Ivo Rittig i exšéf DPP jsou nevinní, rozhodl soud v kauze předražených jízdenek By Autor: Čtk — May 17, 2019 blesk.cz	Save, View Backlinks, View Sharers, Share	972	0	0	0	0	4	972
Nové důkazy z Kypru nepomohly. **Ivo Rittig** je podle soudu nevinen - Seznam Zprávy Sep 13, 2018 seznamzpravy.cz	Save, View Backlinks, View Sharers, Share	275	0	0	0	0	0	275
FOTO Totálně uvolněný **Ivo Rittig** oslavuje osvobození. Blamáž žalobců a zpovykaného redaktora ČT Hynka... May 17, 2019 parlamentnilisty.cz	Save, View Backlinks, View Sharers, Share	222	4	0	0	0	3	226

nes fit

KnowEm and NameChecker



Agenda

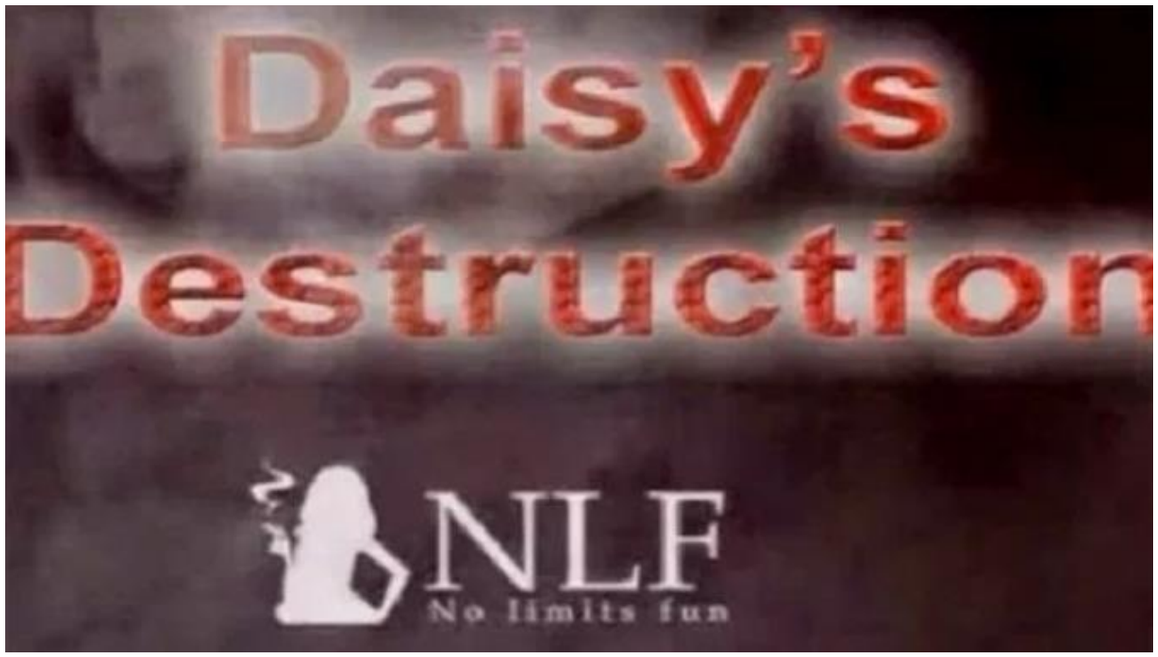
- OSINT
- TOR

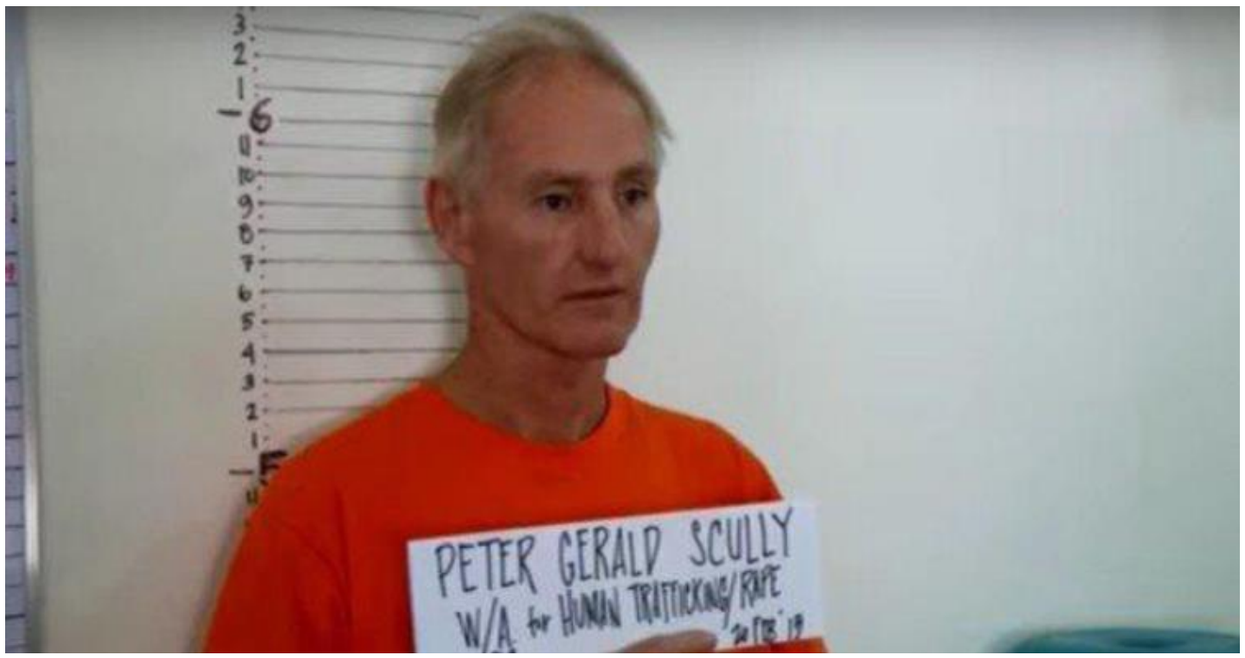
Ecosystem

- Most of TOR sites are botnets
  (hundreds of thousands of visits per day)
- Child abuse sites
  (hundreds of thousands+/day)
- Remainings are marketplaces, hidden wikis, search engines
  (thousands+/day)

Daisys Destruction

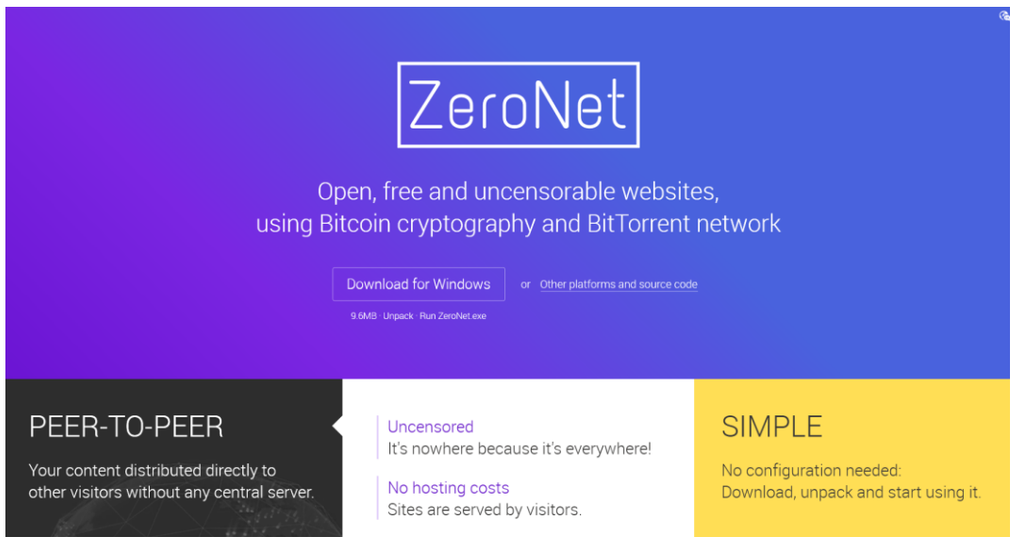
- Daisy's Destruction, which he sold to clients for up to $10,000.
- Made in 2012, the multi-part film is so extreme that it was for some time regarded as an urban legend.
- It features the torture and brutal rape of a number of girls by Scully and some Filipina accomplices; the three main victims were Liza (aged 12), Cindy (11) and Daisy (18 months).
- Peter Gerald Scully put Daisy's Destruction out under his "No Limits Fun" production company, selling it to other people via the dark web. Among those who acquired it was one of the biggest-ever purveyors of child pornography, Scully's fellow Australian Matthew David Graham.

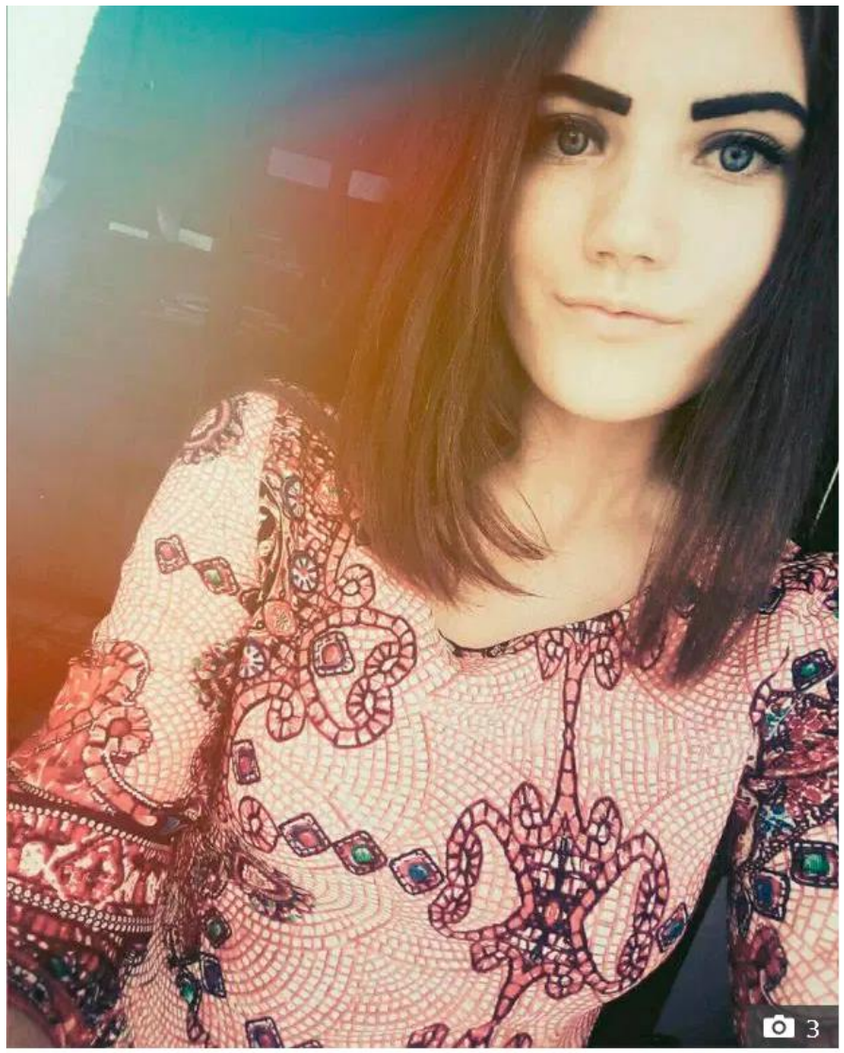




BlueWhale Game

- The "Blue Whale challenge" was reported to be an online "suicide game" aimed at teenagers which set 50 tasks over 50 days
- Ending with winning the game by taking a selfie and committing suicide
- Distributed via ZeroNet





Yulia Konstantinova, 15, joined her friend Veronika in jumping from the roof of a 14-storey block of flats Credit: The Siberian Times

Ports

Table 1
Port-scans of long-lived ($n = 14972$) and short-lived services ($n = 352$).

Port	On-publication	Snapshot	Up < 24hr
22 (ssh)	12.1%	10.59%	–
23 (Telnet)	0.6%	0.09%	–
25/110 (Mail)	1.1%	4.13%	–
53 (DNS)	–	0.05%	–
80 (http)	54.6%	74.16%	51.4%
443 (https)	2.0%	3.61%	–
IRC (all)	1.2%	1.36%	–
3306 (MySQL)	–	0.08%	–
XMPP (all)	–	1.36%	–
8060 (OnionCat)	–	0.89%	–
8080	0.9%	0.41%	–
8333 (Bitcoin)	0.3%	1.0%	–
9878 (Riccochet)	1.1%	0.67%	–
11009 (TorChat)	–	0.37%	–
15441 (Zeronet)	26.1%	0.77%	48.6%

Users and Relays

Relay Search

country:cz

country:cz

Show 100 entries

Advertised

Relay Search

flag:exit country:cz

flag:exit country:cz

Show 10 entries

Advertised

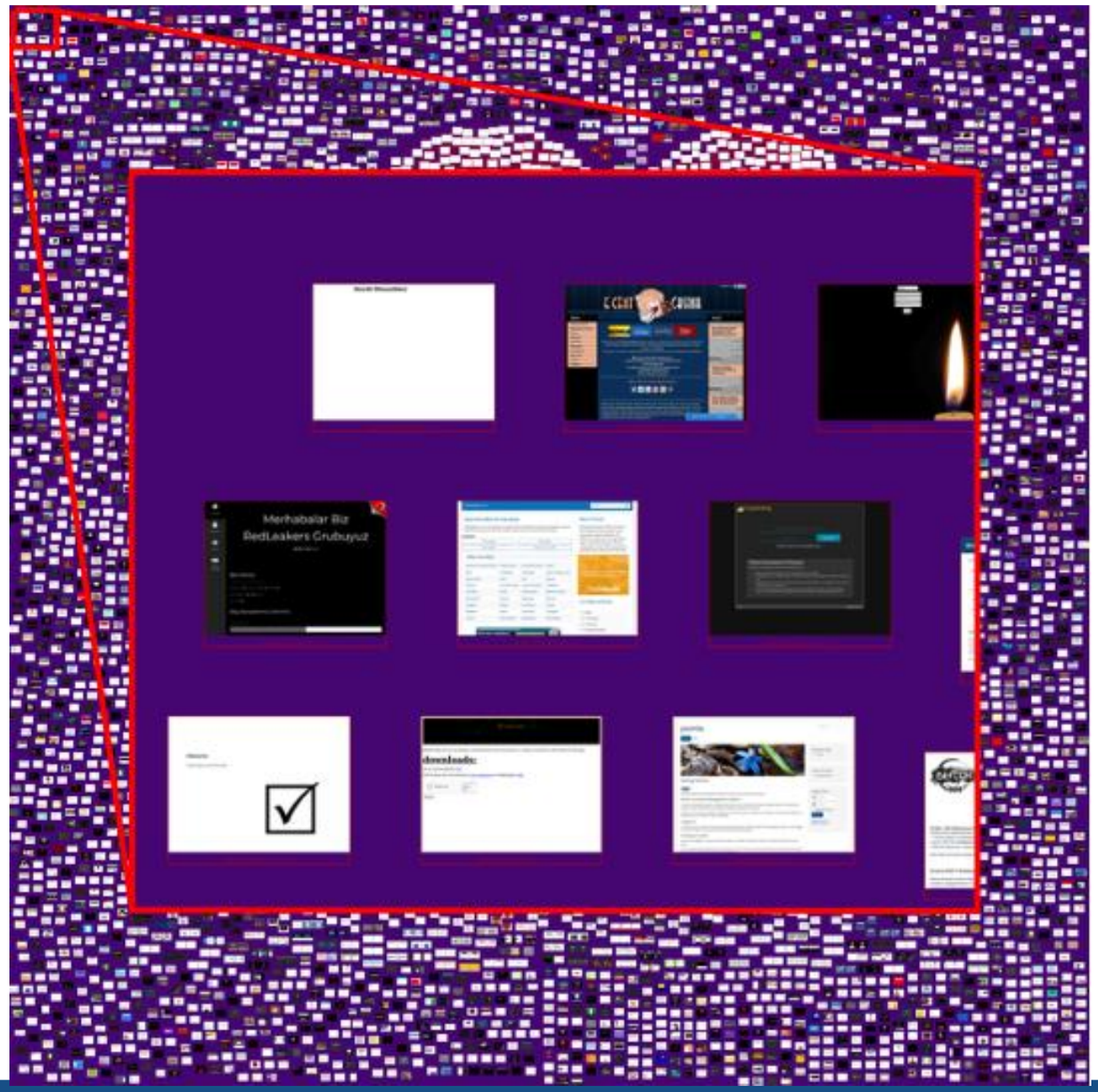
Nickname†	Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
KrlEuBridge (1)	0 B/s	~~6d 7h~~		79.98.77.237	-			9777	0	Relay
brmlab (1)	700 KiB/s	4d 21h		91.146.121.3	-			80	0	Relay
Unnamed (1)	2.97 MiB/s	3d 8h		31.31.74.131	-			443	80	Relay
trooper (1)	2.88 MiB/s	2d 15h		31.31.72.24	-			443	80	Relay
mrkvotor (1)	200 KiB/s	1d 23h		80.79.23.7	-			443	9030	Relay
Total	**6.73 MiB/s**									

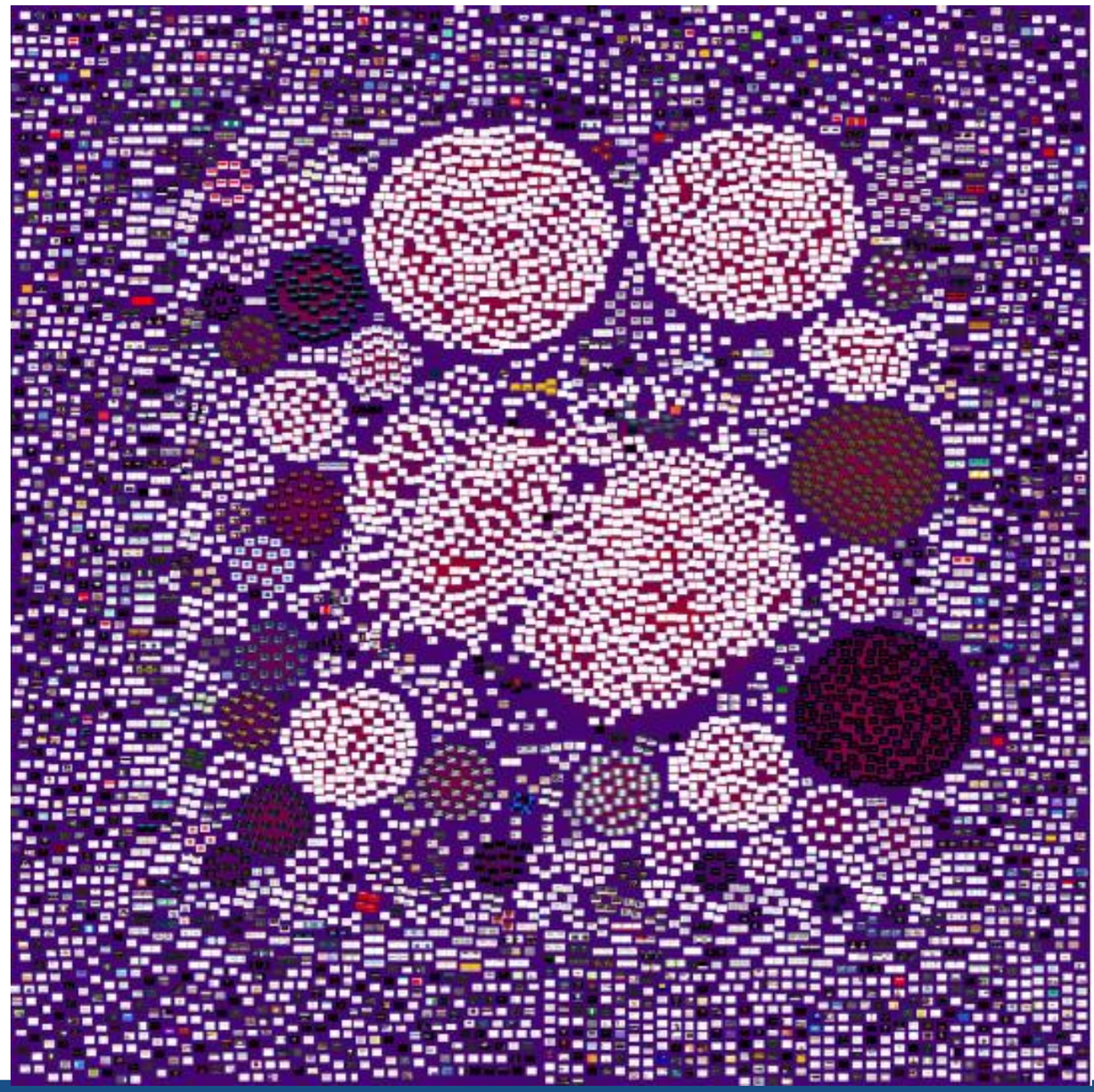
Showing 1 to 5 of 5 entries

	18h							
nuushe (1)	600 KiB/s	87d 20h	80.211.211.72	-		38008	0	Relay
n4lksask972137tor (1)	762.86 KiB/s	76d 18h	62.168.3.212	-		9999	9998	Relay
BlueVenera (1)	473.01 KiB/s	75d 14h	80.211.218.201	-		2681	0	Relay

Hyperion Gray

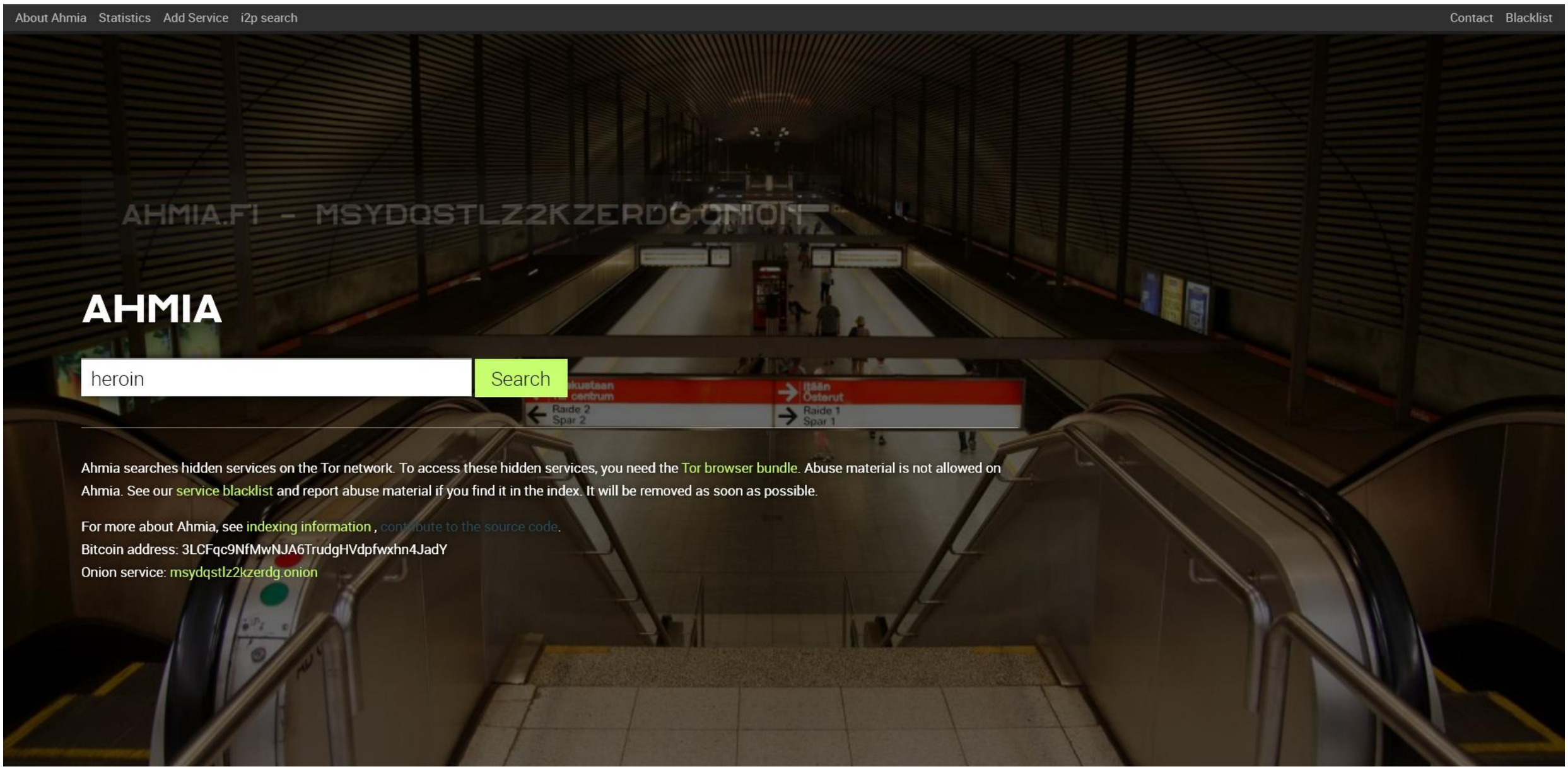
- https://blog.hyperiongray.com/dark-web-map-introduction/





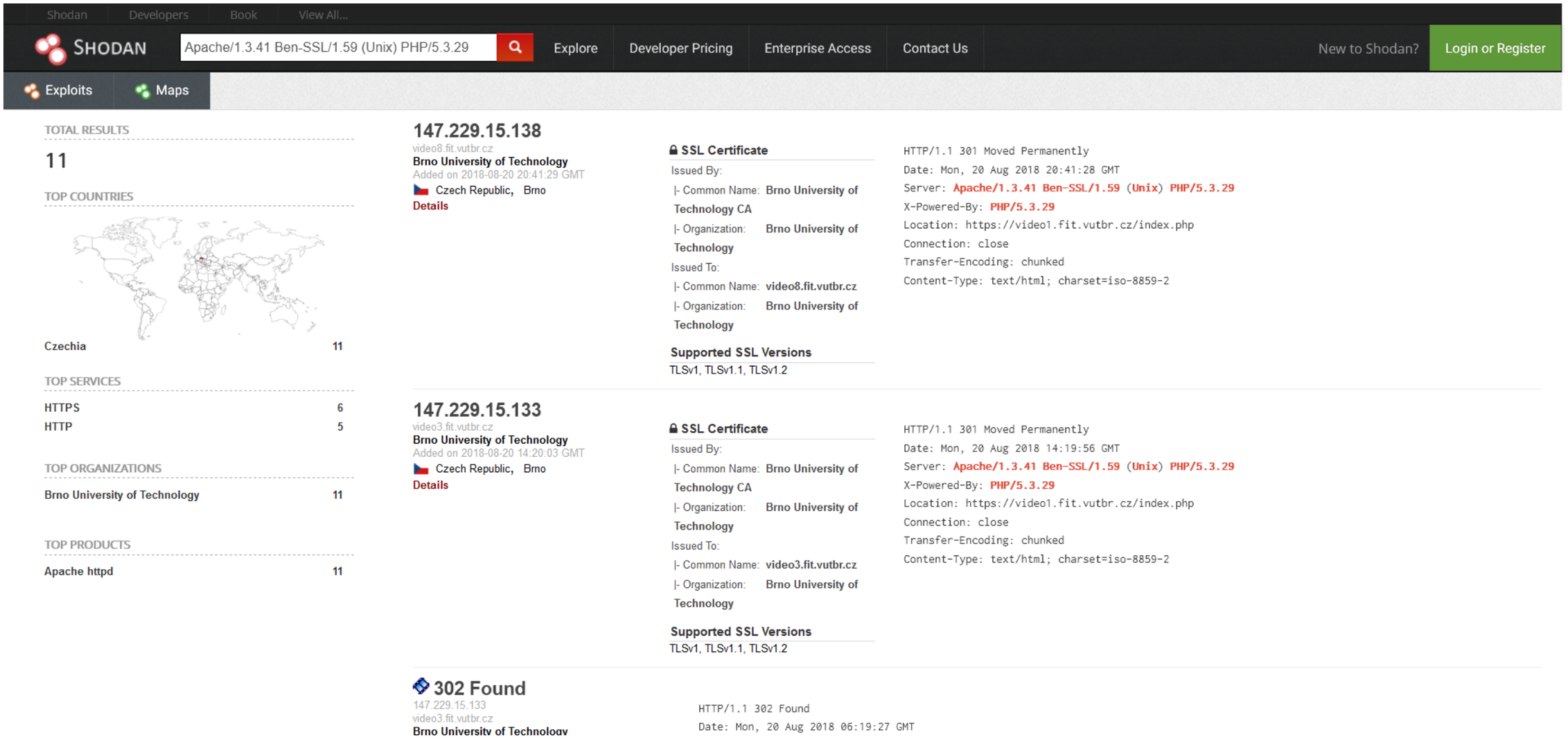
Ahmia

- https://ahmia.fi/



Tracking TOR servers

- https://video3.fit.vutbr.cz/



- https://www.shodan.io/search?query=Apache%2F1.3.41+Ben-SSL%2F1.59+%28Unix%29+PHP%2F5.3.29

TOREATOR

- http://toreator.fit.vutbr.cz/addresses/193.165.189.6/month/
- http://toreator.fit.vutbr.cz/addresses/67.174.243.193/date/2018-08-20/

Result

Nickname seele published at 2018-08-19 16:54:56

- IPv4 address 67.174.243.193 port 9001
- DNS reverse name c-67-174-243-193.hsd1.ca.comcast.net queried at
  - 2018-08-19 21:10:00
  - 2018-08-19 22:10:00
  - 2018-08-19 23:10:00
- Server flags in Tor network Fast, Running, Stable, V2Dir, Valid, Tor exit policy reject 1-65535
- MaxMind Geolocation:
  - from 2018-08-07 00:00:00:
    - network: 67.174.240.0/22
    - continent: North America
    - country code: US
    - country: United States
    - country part: California
    - city: Sunnyvale
    - time zone: America/Los_Angeles
    - inside EU: False
- MaxMind autonomous system number:
  - from 2018-08-14 00:00:00:
    - AS network: 67.160.0.0/11
    - AS number: 7922
    - AS organization: Comcast Cable Communications, LLC
- Valid in consensuses after ("2018-08-19 21:00:00",), fresh until ("2018-08-20 00:00:00",), valid until ("2018-08-20 02:00:00",)
- Tor software version: Tor 0.3.3.9
- Node bandwidth: {'Bandwidth': '25'}
- Identity: AAoQ1DAR6kkoo19hBAX5K0QztNw
- Digest: wA8aSjn9T+3usgWeGsWDIM9Y74E
- Dirport: 0
- Supported protocols: ('Cons=1-2', 'Desc=1-2', 'DirCache=1-2', 'HSDir=1-2', 'HSIntro=3-4', 'HSRend=1-2', 'Link=1-5', 'LinkAuth=1,3', 'Microdesc=1-2', 'Relay=1-2')

Nickname seele published at 2018-08-19 16:54:56

- IPv4 address 67.174.243.193 port 9001

Alpha Bay


THIS HIDDEN SITE HAS BEEN SEIZED
Since July 4, 2017
as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol
in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.

Dream Market

Dream Market
lchudifyeqm4ldjj.onion
Established 2013

Register Login 2FA Login

Onion mirrors

uffti3lhacanefgy.onion
verified

wdsgtsqkk5sk5zmqr4pc2lqd
oxfwgrjvw2i55kloczhqq3nvr3b
m3wyd.onion
jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

Choose one of the links above if the site is loading too slow.

Dark Dode

This market is shutting down on 04/30/2019 and is transferring its services to a partner company, onion address: weroidjkazxqds2l.onion (currently offline, opening soon)

Questions?

veselyv@fit.vutbr.cz

Děkuji za pozornost…