



nes  fit

ISS News

Vladimír Veselý
2019-09-09



Agenda

- OSINT
- TOR

Anders Breivik

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

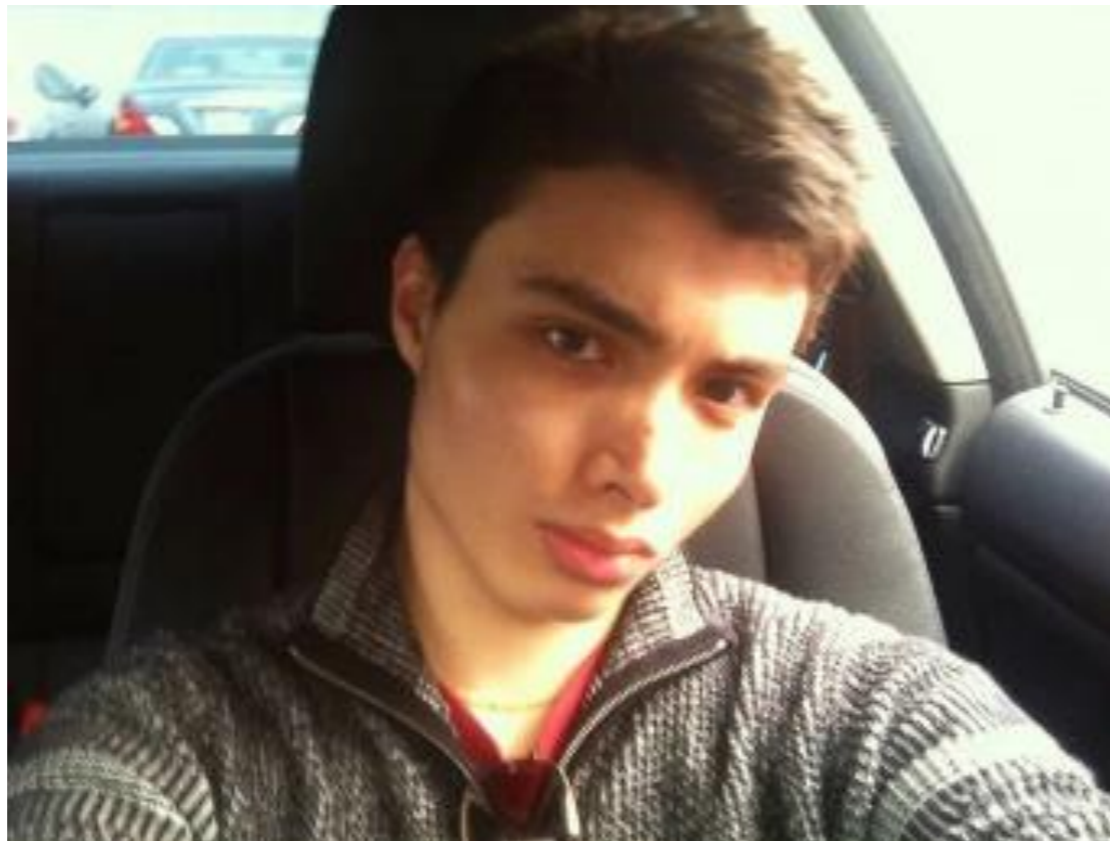
| | |
|--------------------|---|
| Location | Oslo and Utøya, Norway |
| Coordinates |  59°54′54″N 10°44′48″E |
| Date | 22 July 2011 Oslo: 15:25 ^[1] CEST Utøya: 17:22–18:34 CEST ^{[2][3]} (UTC+02:00) |
| Target | Labour Party ^{[4][5]} |
| Attack type | Car bomb, mass shooting, terrorism |
| Weapons | 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

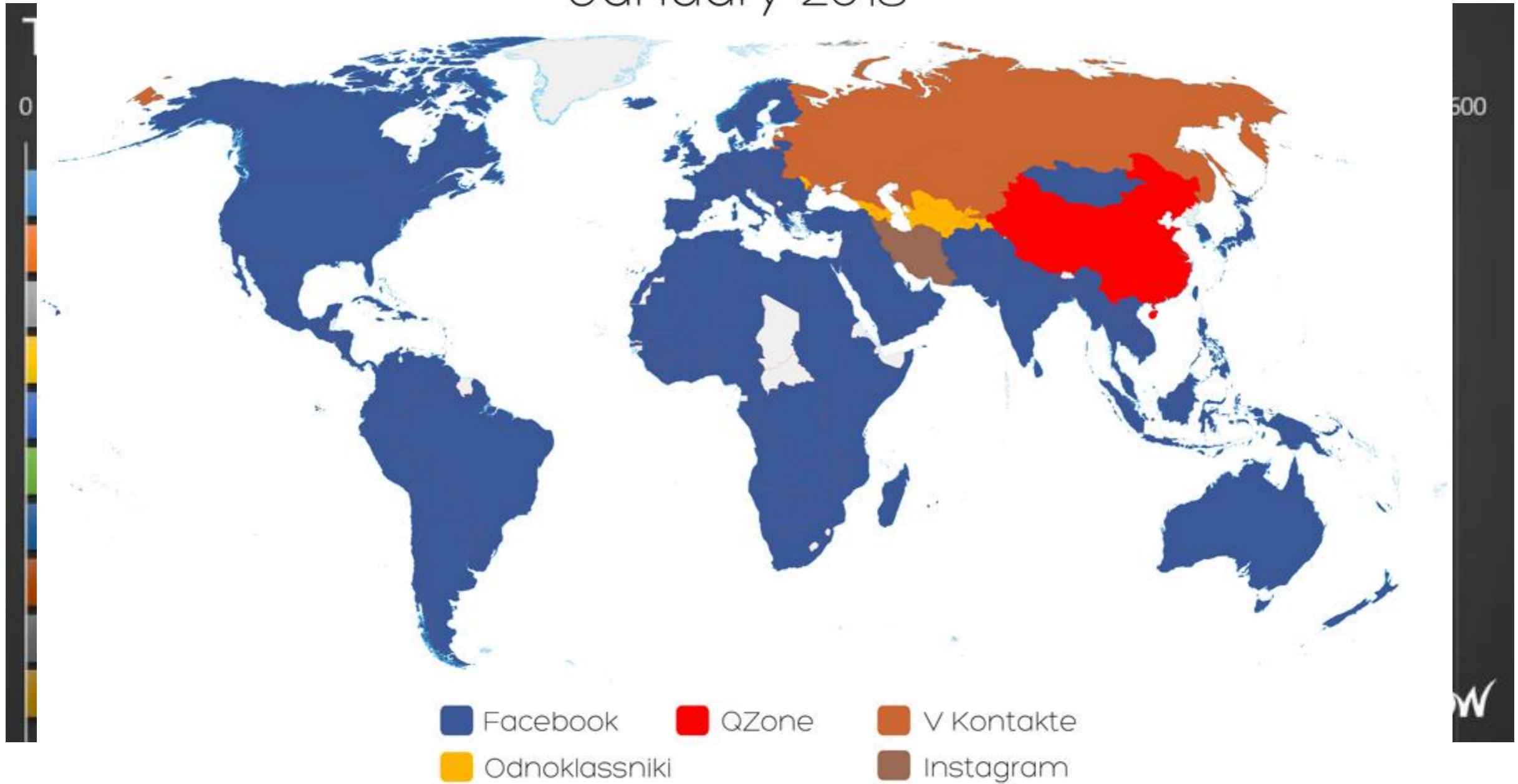
Ismaaiyl Abdullah Brinsley

- 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




credits: Vincenzo Cosenza vincos.it

license: CC-BY-NC

source: Alexa/SimilarWeb

Tweet Deck




1 **User** @Rittiglvo

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...



2 9

Ivo Rittig @Rittiglvo Aug 10
A doprdele 🤔🤔🤔🤔

Dallas Stars @dallasstars93
Tak tahle atrakce není pro stary...
twitter.com/cctv_idiots/st...
twitter.com/dallasstars93/status/113...

2 1 6

Ivo Rittig @Rittiglvo Jul 30
Replying to @JackyDanielsu
Promin promin všem se omlouvám se slovem soudruzi jsem se potkával 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.

1 1

David Michal @michaldmsb Aug 7
Replying to @iROZHLAScz @OndejGolis
Ja si myslim, ze Vas soudce Zelenka spravne a chytre vyuzil ke konfliktu toho spolku @UnieSZ se skutecnou justici, tzn. SOUDY 👍⚖️
[#babakovakarol](https://twitter.com/babakovakarol) #msblegal

1

David Michal @michaldmsb Jun 21
Same skvele uspechy @VSZ_Praha 🤔🤔
[#babakovakarol](https://twitter.com/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...](https://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](https://fb.com/LI) twitter.com/surveillance...
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

msb legal rittig

SEARCH SETTINGS email alerts

Set up Free [email alerts](#) or star

FILTERS:

Sort by: Date

ANALYTICS: Mentions: **119**
Users: **54**
Sentiment: **9:1**

Enable **monitoring** to start collecting all mentions history and get live notifications

SEARCH TIPS

Check up exact phrase match
"msb legal rittig"

Select language for more relevant results.

Select

cs.wikipedia.org
Posted 08:21 09 Sep 2019

MSB Legal v.o.s. (do března 2012 Šachta & Partners v.o.s., do prosince 2004 ... Nejznámějším klientem kanceláře je kontroverzní podnikatel Ivo Rittig – JUDr.

[MSB Legal – Wikipedie](#)

[link](#)

www.e15.cz
Posted 08:21 09 Sep 2019

U Rittigových advokátů v MSB Legal zasahuje policie. Domáci ... Za tunelování Oleo Chemical čeká bývalé majitele vězení, Rittig vyvážl. Aktualizováno. Domáci ...

[MSB Legal | E15.cz](#)

[link](#)

hr-hr.facebook.com
Posted 08:21 09 Sep 2019

Advokátka Ivo Rittiga Karolína Babáková z advokátní kanceláře MSB Legal (dříve Šachta Partners) vzkázala, že Ivo Rittig je připraven prokázat, že se na žádné ...

[Myslíte si, že Ivo Rittig dorazí dne... - Nadační fond proti ...](#)

[link](#)

www.facebook.com
Posted 08:21 09 Sep 2019

2 likes. MSB Legal v.o.s. (do března 2012 Šachta & Partners v.o.s., do prosince 2004 ... podnikatel Ivo Rittig – JUDr.

[MSB Legal - Local Business | Facebook](#)

[link](#)

www.facebook.com
Posted 08:21 09 Sep 2019

Ivo Rittig zažaloval Fond na ochranu osobnosti a požadoval odstranění informací ... Poté, kdy byla zamítnuta jak žaloba Ivo Rittiga, tak návrh MSB Legal (o obou ...

[Další vývoj v kauze jízdenek DPP Poté,... - Nadační fond proti ...](#)

[link](#)

www.facebook.com
Posted 08:21 09 Sep 2019

Když mě pověřil klient prezentovat fakta, že advokáti z MSB Legal (dříve Šachta ... ČAK má ke spravedlnosti asi tak blízko jako Ivo Rittig k titulu filantrop roku.

de-de.facebook.com
Posted 08:21 09 Sep 2019

... v pražském dopravním podniku, v níž je hlavním aktérem lobbista Ivo Rittig. ... Stublej pracuje v advokátní kanceláři MSB Legal, dříve Šachta & Partners.

[Forbes Česko - Marek Stublej rezignoval na svůj post ...](#)

[link](#)

hi-in.facebook.com
Posted 08:21 09 Sep 2019

Žaloba Ivo Rittiga se zamítá v plném rozsahu a Ivo Rittig je povinen uhradit náklady řízení NFPK. Právnička Šachta Partners (MSB Legal) se nicméně proti ...

[NFPK dnes vyhrál řízení s Ivo Rittigem a... - Nadační fond proti ...](#)

[link](#)

hi-in.facebook.com
Posted 08:21 09 Sep 2019

Právníci z advokátní kanceláře MSB Legal si stěžovali na výroky ve vysílání Českého ... Ivo Rittig bude muset NFPK uhradit i veškeré náklady na soudní řízení.

[NFPK s Láskou Nadační fond proti... - Nadační fond proti korupci](#)

[link](#)

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

Content Analyzer

Search Analysis

Ivo Rittig

Search

Save Search

Export

Total Results: 15

How to run an Advanced Search

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



Nové důkazy z Kypru nepomohly. Ivo Rittig je podle soudu nevinen - Seznam Zprávy

Sep 13, 2018
seznamzpravy.cz

- Save
- View Backlinks
- View Sharers
- Share



FOTO Totálně uvolněný **Ivo Rittig** oslavuje osvobození. Blamáž žalobců a zpovynkaného redaktora ČT Hynka...

May 17, 2019
parlamentnilisty.cz

- Save
- View Backlinks
- View Sharers
- Share



KnowEm and NameChecker

Information

about.me Available **ALLMYFAVES** Available **appearedo** Available **ask.fm** Available
ASK ME Available **bloglovin'** Available **calendly** Available **DOJO PRESS** Available
Welcome to Edmodo Available **FlightAware** Available **FLIPBOARD** Available **Gravatar** Available
huffduffer Available
JustPaste.it Available
MOUTHSUT.com Available
pearltrees Available
rrather Available
Trello Available
zotero Available

namecheckr kvetak

Check domain & social username availability across multiple networks. [Need Help?](#)

| | | | | | | |
|---------------|---------------|---------|-----------|------------|------------|-----------|
| Domain (.com) | Facebook | Twitter | Tumblr | Reddit | Slack | instagram |
| Domain (.net) | Myspace | Youtube | meetup | Pinterest | spotify | Dribbble |
| Github | Domain (.org) | Vimeo | Elo | Feedburner | Foursquare | last.fm |
| me about.me | Domain (.io) | Flickr | Wordpress | Blogger | Venmo | Cash App |

Agenda

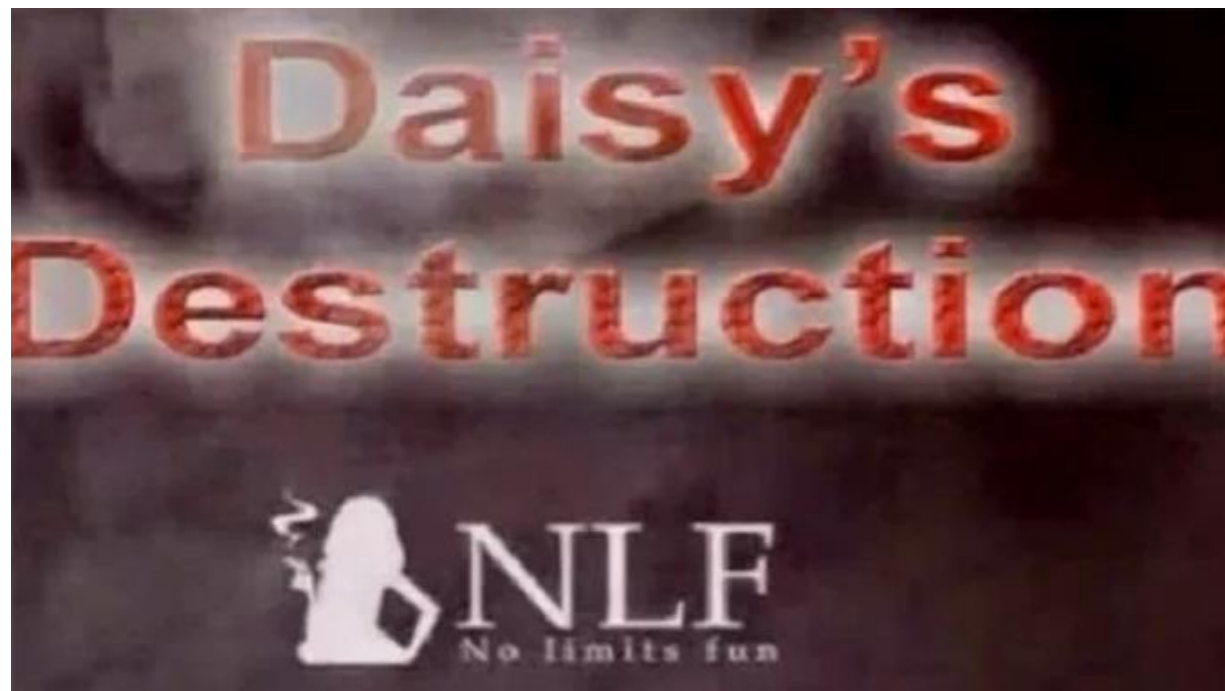
- OSINT
- TOR

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)

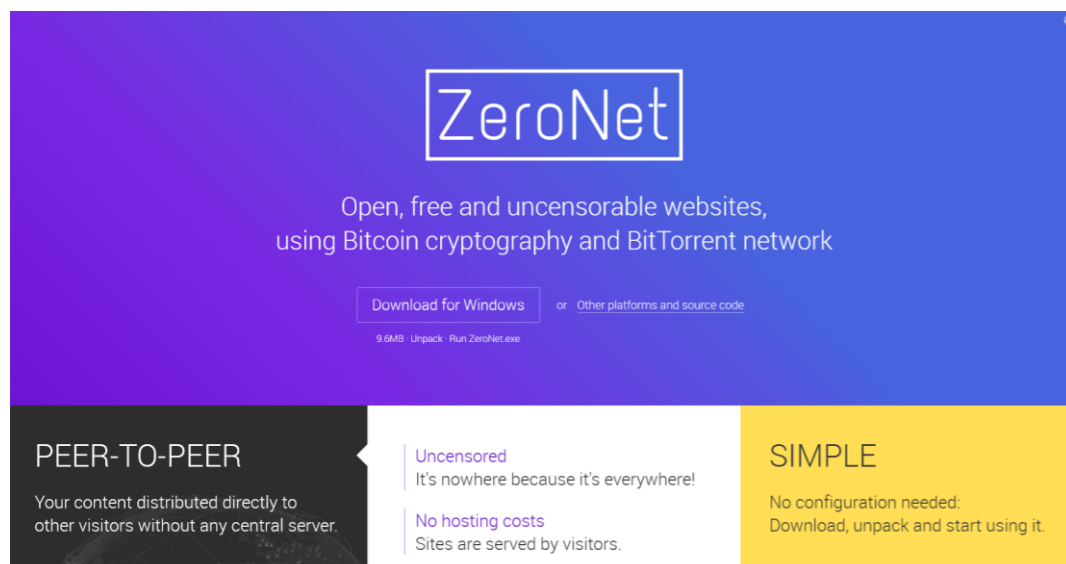
Daisy's Destruction

- 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 (Ricochet) | 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 entries

Advertised

flag:exit country:cz   

Relay Search

flag:exit country:cz

Show entries

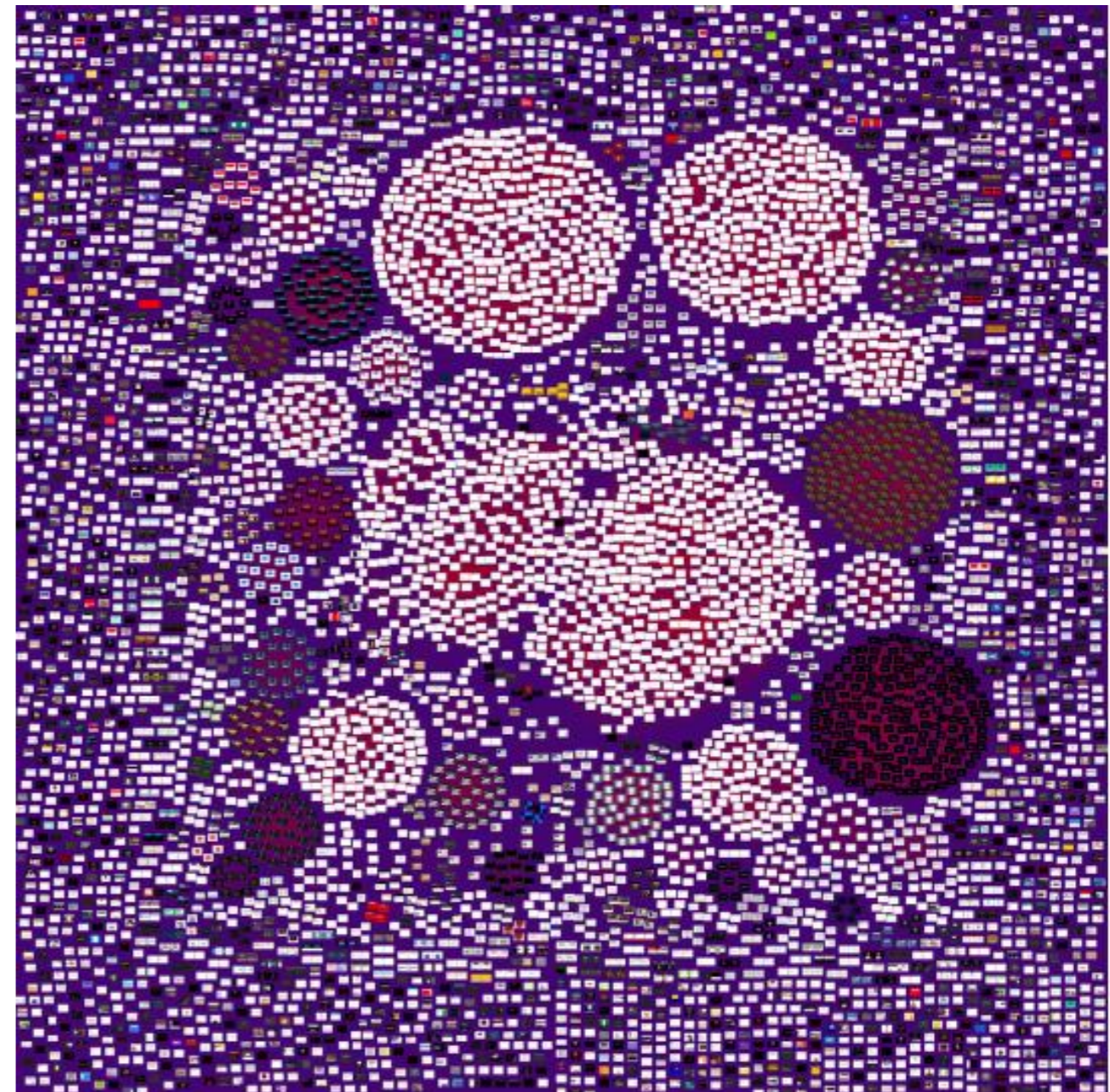
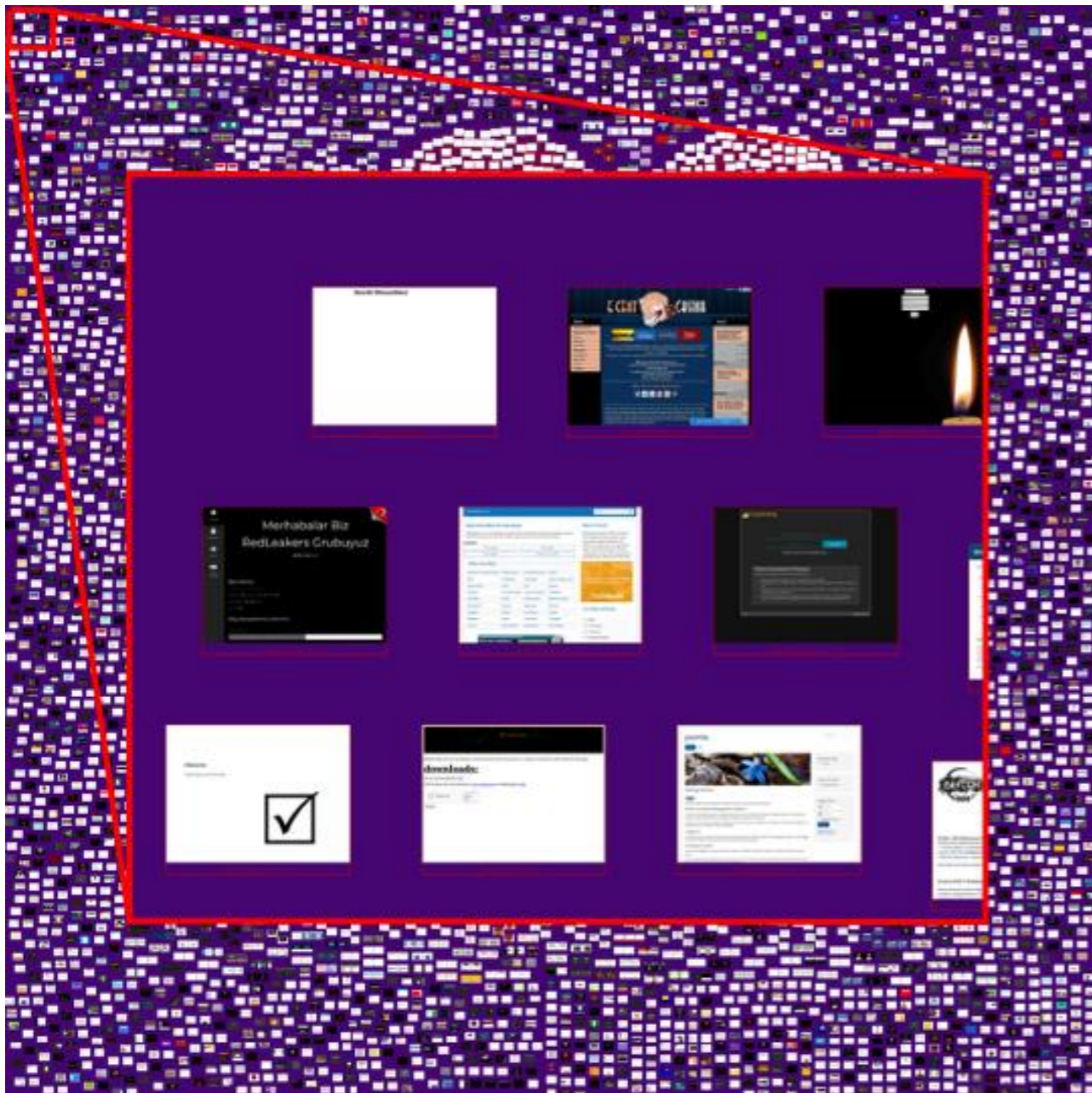
| Nickname [†] | Advertised Bandwidth | Uptime | Country | IPv4 | IPv6 | Flags | Add. Flags | ORPort | DirPort | Type |
|-----------------------|----------------------|--------|---------|--------------|------|-------|------------|--------|---------|-------|
| KrlEuBridge (1) | 0 B/s | 6d 7h | | 79.98.77.237 | - | | | 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

| | | | | | | | | | | |
|-----------------------|--------------|---------|--|----------------|---|--|--|-------|------|-------|
| 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 |

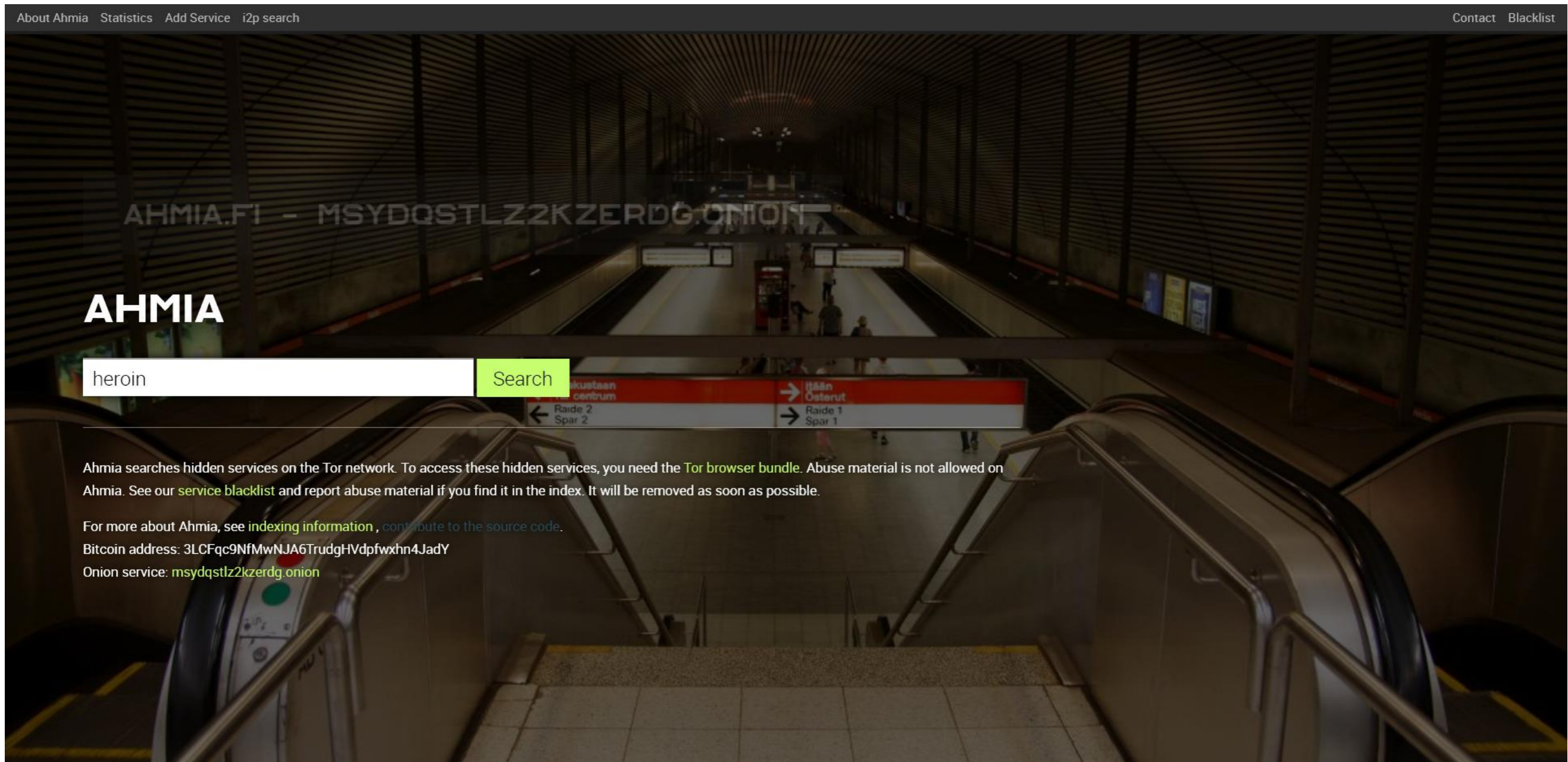
Hyperion Gray

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



Ahmia

- <https://ahmia.fi/>



The screenshot shows the Ahmia website interface. At the top, there is a navigation bar with links for "About Ahmia", "Statistics", "Add Service", "i2p search", "Contact", and "Blacklist". The main content area features the Ahmia logo and a search bar containing the word "heroin". A green "Search" button is positioned to the right of the search bar. Below the search bar, there is a paragraph of text: "Ahmia searches hidden services on the Tor network. To access these hidden services, you need the [Tor browser bundle](#). Abuse material is not allowed on Ahmia. See our [service blacklist](#) and report abuse material if you find it in the index. It will be removed as soon as possible." Below this paragraph, there are three lines of text: "For more about Ahmia, see [indexing information](#), [contribute to the source code](#)." "Bitcoin address: [3LCFqc9NfMwNJA6TrudgHVdpfwxhn4JadY](#)" and "Onion service: [msydstlz2kzerdg.onion](#)". The background of the website is a photograph of a subway station with escalators and a sign that reads "Astmia.fi - msydstlz2kzerdg.onion".

Tracking TOR servers

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

The screenshot shows the Shodan search interface with the query 'Apache/1.3.41 Ben-SSL/1.59 (Unix) PHP/5.3.29'. The results are filtered to show 11 total results, all from the Czech Republic, specifically from Brno University of Technology. Two results are highlighted:

- 147.229.15.138**
video8.fit.vutbr.cz
Brno University of Technology
Added on 2018-08-20 20:41:29 GMT
Czech Republic, Brno
Details
- 147.229.15.133**
video3.fit.vutbr.cz
Brno University of Technology
Added on 2018-08-20 14:20:03 GMT
Czech Republic, Brno
Details

Each highlighted result includes an SSL Certificate section and a 'Supported SSL Versions' section (TLSv1, TLSv1.1, TLSv1.2). The SSL Certificate sections show the following details:

- 147.229.15.138:** Issued By: Brno University of Technology CA; Issued To: video8.fit.vutbr.cz
- 147.229.15.133:** Issued By: Brno University of Technology CA; Issued To: video3.fit.vutbr.cz

The '302 Found' section shows a redirect from 147.229.15.133 to video3.fit.vutbr.cz.

Summary statistics from the left sidebar:

- TOTAL RESULTS: 11
- TOP COUNTRIES: Czechia (11)
- TOP SERVICES: HTTPS (6), HTTP (5)
- TOP ORGANIZATIONS: Brno University of Technology (11)
- TOP PRODUCTS: Apache httpd (11)

- <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 consensus 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



Dream Market

Dream Market
Ichudifyeqm4ldjj.onion
Established 2013

Register

Login

2FA Login



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)



Onion mirrors

[uffti3lhacaneqfy.onion](#)

verified 

[wdsqtsqkk5sk5zmqr4pc2lqd
oxfwgrjvw2i55kloczhqq3nvr3b
m3wyd.onion](#)

[jd6yhuwcivehvd4.onion](#)

[t3e6ly3uoif4zcv2.onion](#)

[7ep7acrkunzdcw3l.onion](#)

[vilpaqbrnvizecjo.onion](#)

[igyifrhvxq33sy5.onion](#)

[6qlocfg6zq2kyacl.onion](#)

[x3x2dwb7jasax6tq.onion](#)

[bkjcpa2klkkmowwq.onion](#)

[xytjqcfendzeby22.onion](#)

[nhib6cwhfsoyiugv.onion](#)

[k3pd243s57ftnpa.onion](#)

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

Dark Mode



Questions?

veselyv@fit.vutbr.cz

Děkuji za pozornost...