The Zeitgeist of Darknet

OWASP Czech Chapter Meeting

14th November 2018

Ing. Martin Klubal

Senior IT Security Specialist

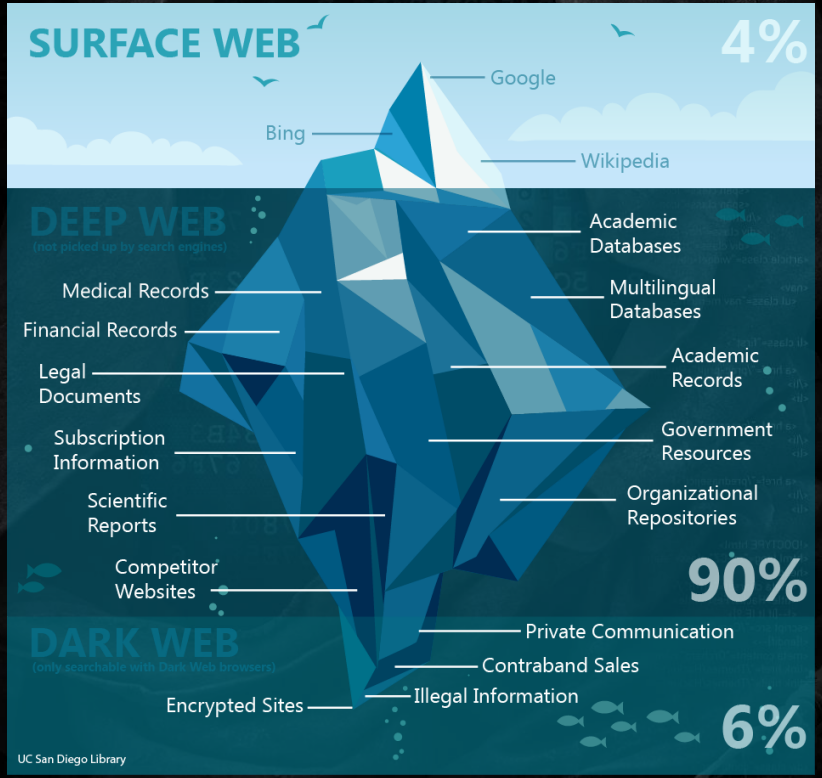
info@martinklubal.cz

Content

- Terminology
- Tor News in 2018
  - Next Gen Onion Services
  - Tor Browser for Android
- Statistics
- Vulnerabilities
- Seizure & Conviction
- Popular Hidden Services
- DEMO: Tor Real Hacking

Terminology

- Clearnet/Surface web
  - https://www.google.com/
  - http://crdclub.su/
- Darkweb (Darknet)
  - Hidden Wiki
  - Silk Road
- Deepweb
  - Invite Only Sites



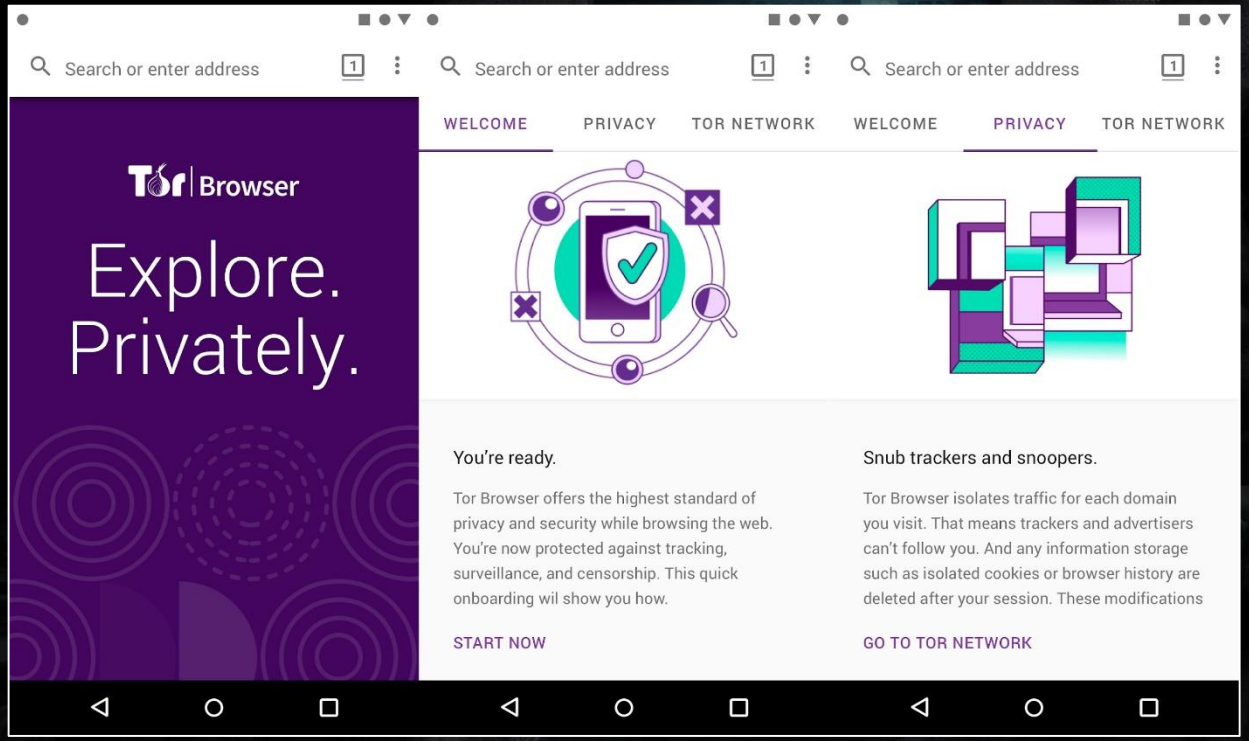
Next Gen Onion Services aka prop224

- Better crypto
- Improved directory protocol
- Better onion address security against impersonation
- More extensible introduction/rendezvous protocol
- A cleaner and more modular codebase
- Onion v3 Addresses
  - 56 characters long

vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd**.onion**

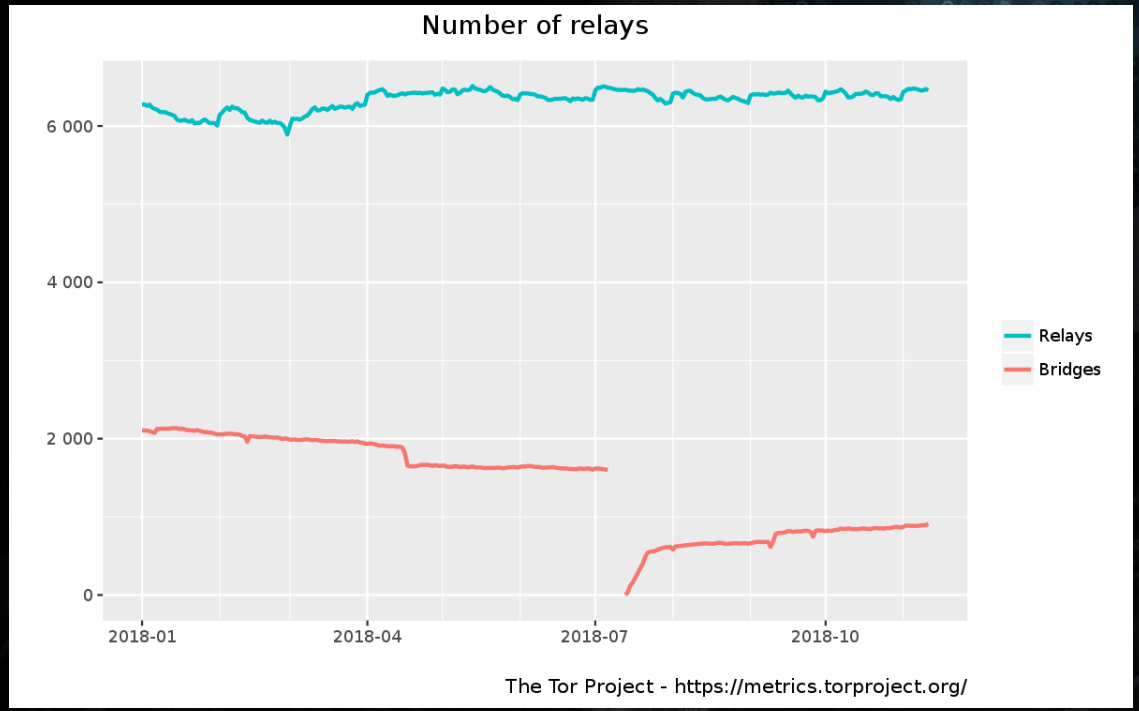
Tor Browser for Android

- Google Play (Alpha)
  https://play.google.com/store/apps/details?id=org.torproject.torbrowser_alpha
- Alternatives
  - Orfox (don‘t use anymore)
  - Onion Browser (iOS)

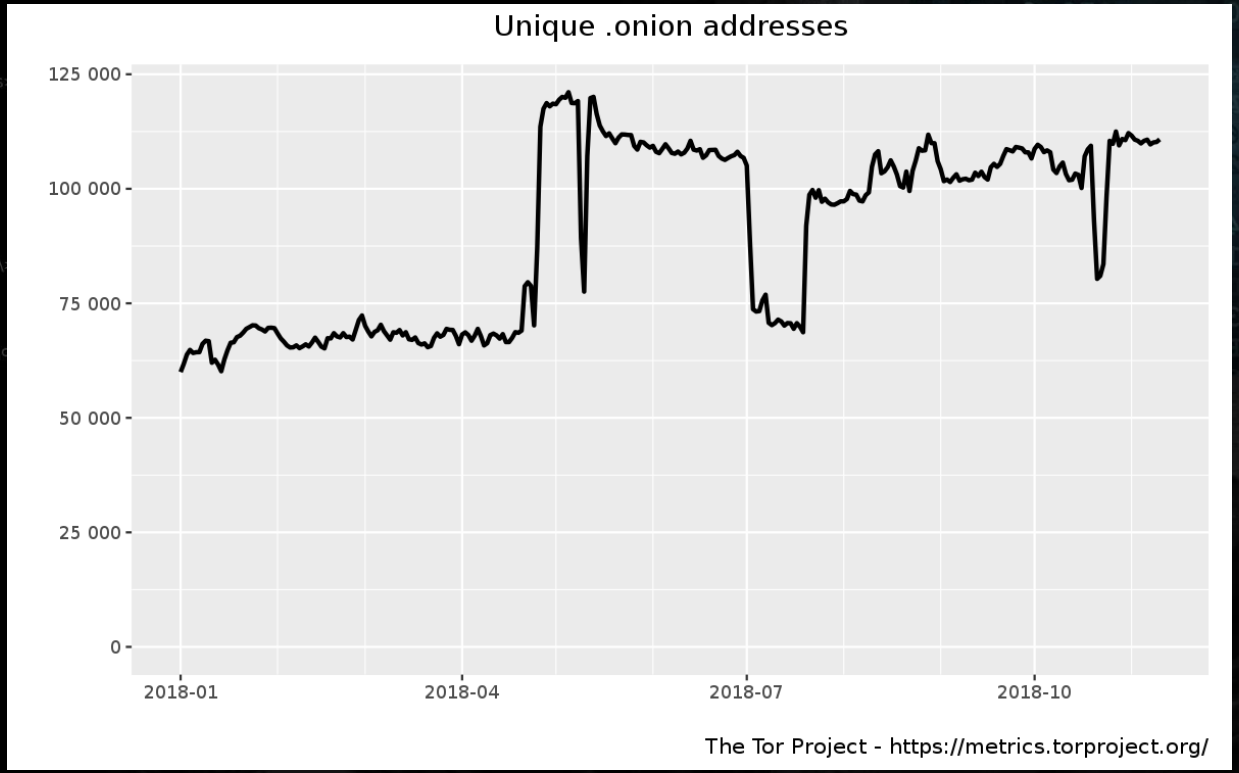


Statistics

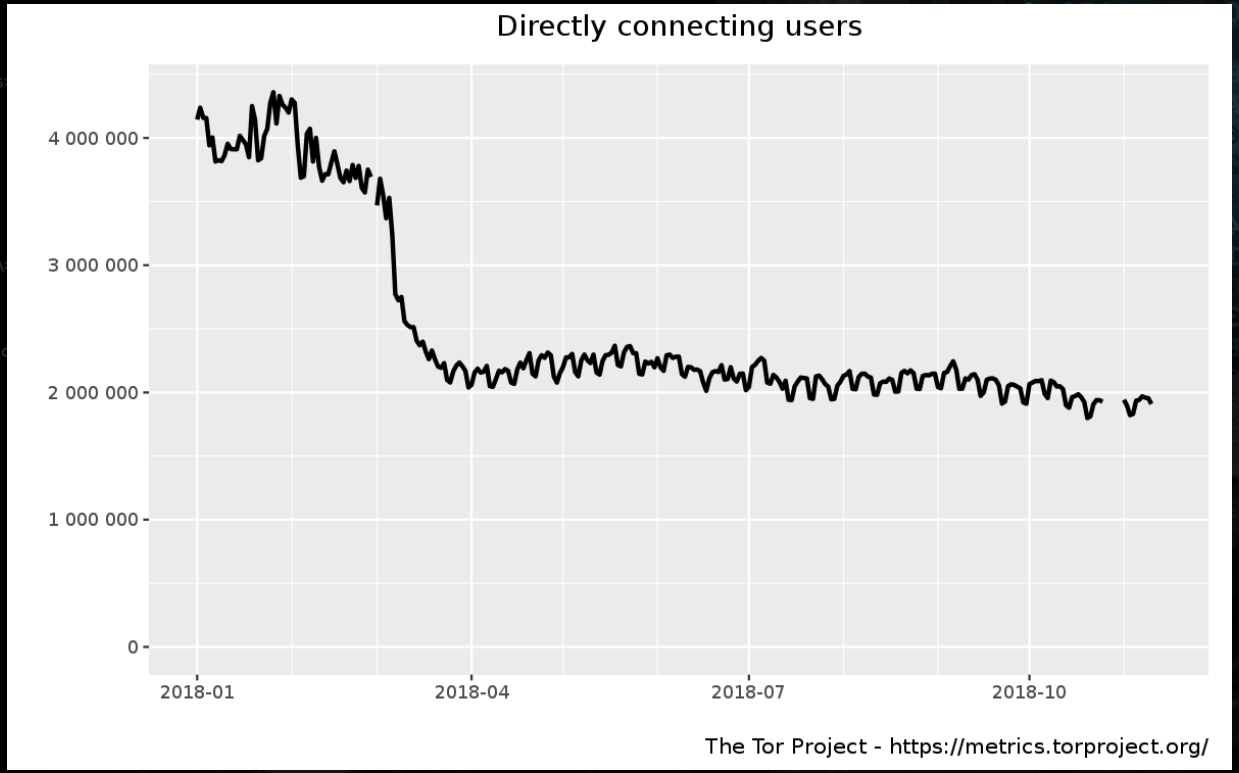
- Atlas – List of relays
  - https://atlas.torproject.org/



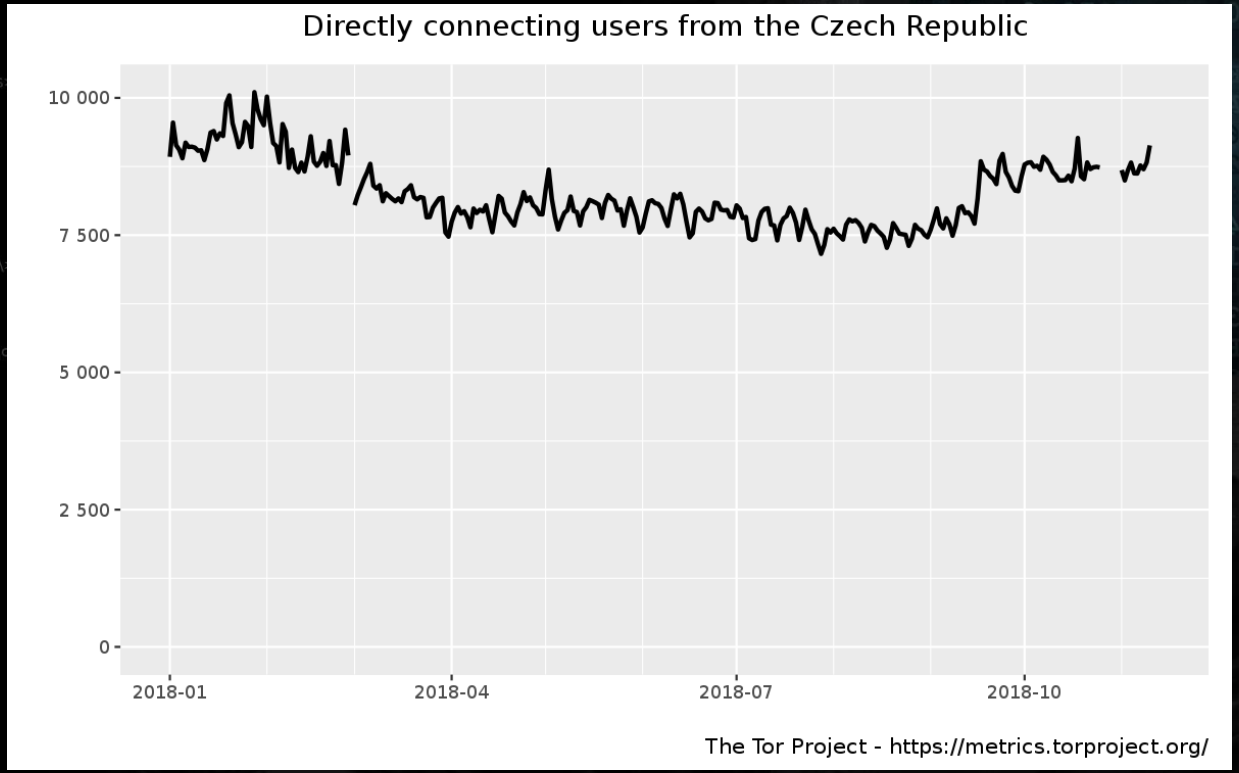
Statistics


Unique .onion addresses
125 000
100 000
75 000
50 000
25 000
0
2018-01
2018-04
2018-07
2018-10
The Tor Project - https://metrics.torproject.org/

Statistics


Directly connecting users
4 000 000
3 000 000
2 000 000
1 000 000
0
2018-01
2018-04
2018-07
2018-10
The Tor Project - https://metrics.torproject.org/

Statistics


Directly connecting users from the Czech Republic
10 000
7 500
5 000
2 500
0
2018-01
2018-04
2018-07
2018-10
The Tor Project - https://metrics.torproject.org/

Statistics

- Top 10 countries by relay users in 2018
  - Germany 466948 (18.68 %)
  - USA 403368 (16.14 %)
  - UAE 292873 (11.72 %)
  - Russia 250015 (10.00 %)
  - France 102353 (4.10 %)
  - Ukraine 98135 (3.93 %)
  - Indonesia 83692 (3.35 %)
  - UK 63145 (2.53 %)
  - Netherlands 55173 (2.21 %)
  - India 43275 (1.73 %)

Vulnerabilities

- Tor Browser 0-Day Exploit
  - version 7.x
  - vulnerability in the NoScript plugin
  - JavaScript execution in Safest Security Level
    - Tor users deanonymization
  - patched in the latest branch 8.x

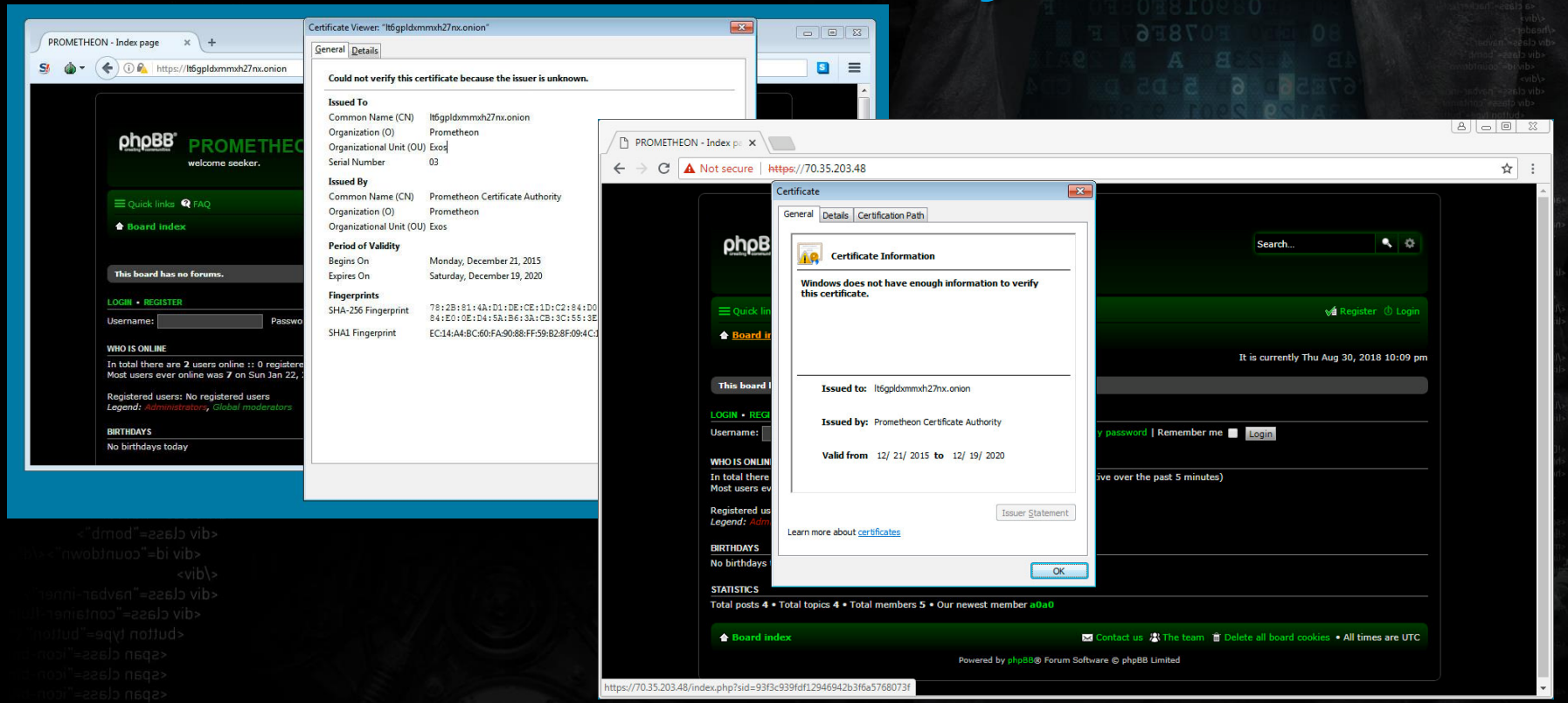
https://twitter.com/Zerodium/status/1039127214602641409

Vulnerabilities

- Guard Discovery
  - the most serious threat of the v3 onion services
  - lots of relays under the attacker control required
    - Hidden Services & Tor users deanonymization
  - Patched through the Vanguards Add-On
    - not a part of the Tor core yet

https://blog.torproject.org/announcing-vanguards-add-onion-services

SSL Certificate Deanonymization



Vulnerabilities

- SSL Certificate Deanonymization
  - Use Shodan
- DigiCert.com issues trusted .onion certs
- SSL certs are redundant in Tor

https://twitter.com/ydklijnsma/status/1025796349541769217

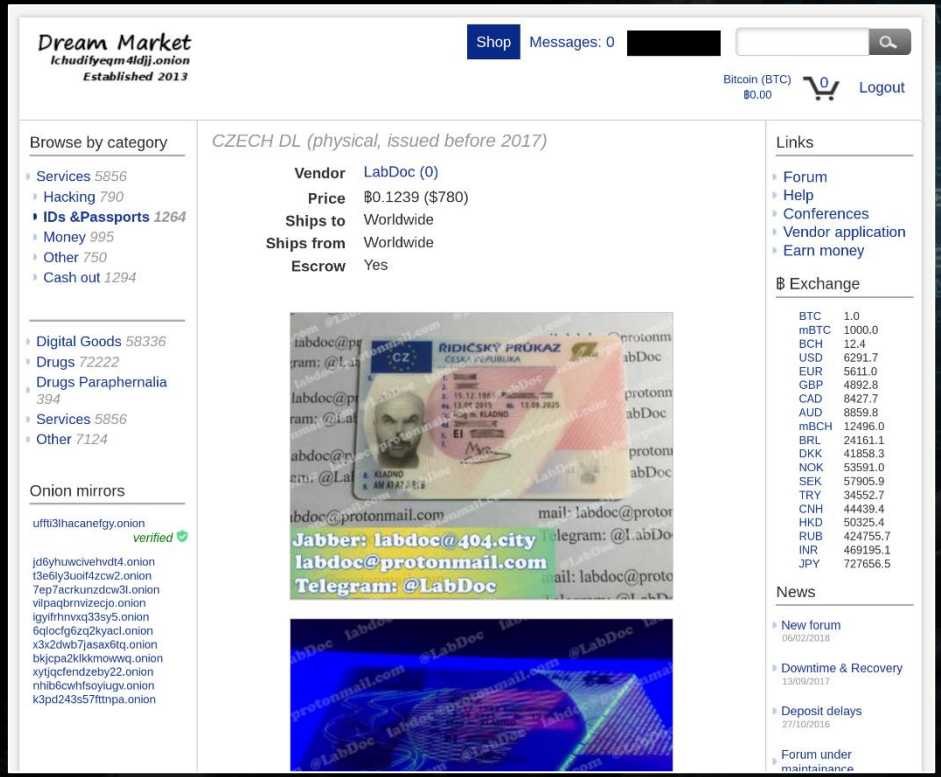
Seizure & Conviction

- No significant Hidden Service seized
- Conviction
  - Gary Davis (Irish)
    - Silk Road admin
    - Pleaded guilty to drug trafficking (up to 20 years)
  - Gal Vallerius (French)
    - Dream Market admin
    - Pleaded guilty to drug trafficking/launder money (20 years)

Popular Hidden Services

- Dream Market
  - http://uffti3lhacanefgy.onion/
  - Black Market
  - online from November 2013

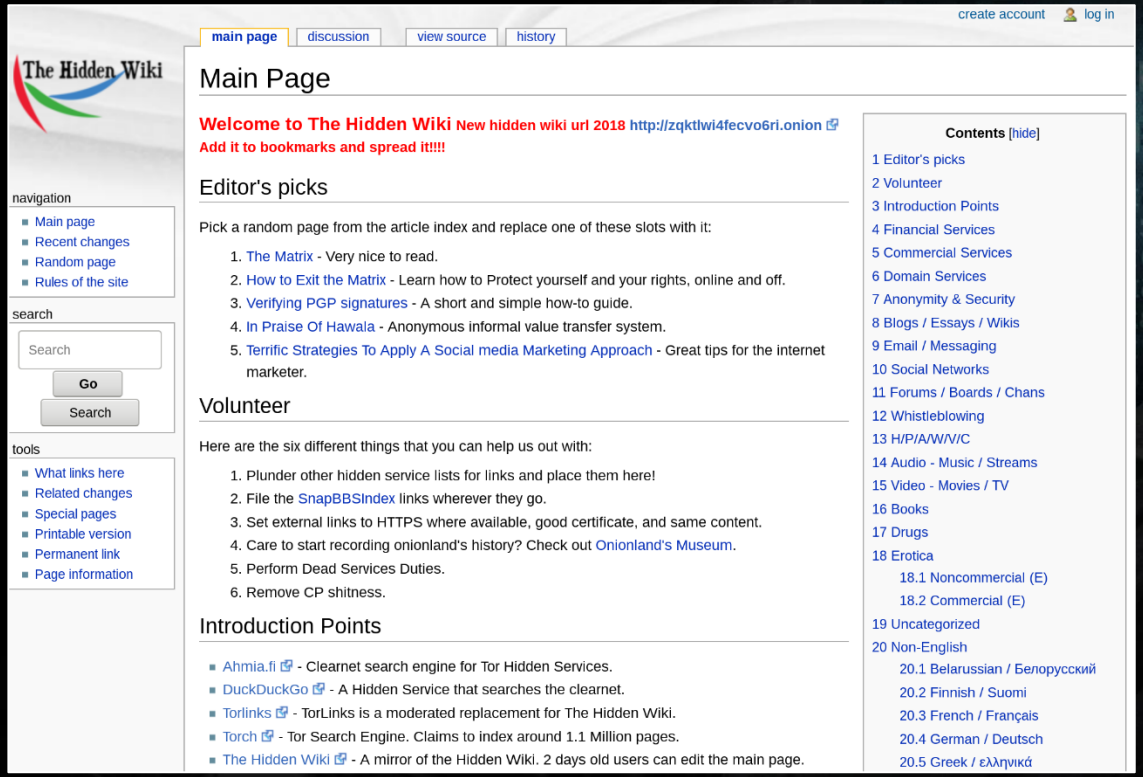
Dream Market



Popular Hidden Services

- The Hidden Wiki
  - http://zqktlwi4fecvo6ri.onion/
  - Directory of Links

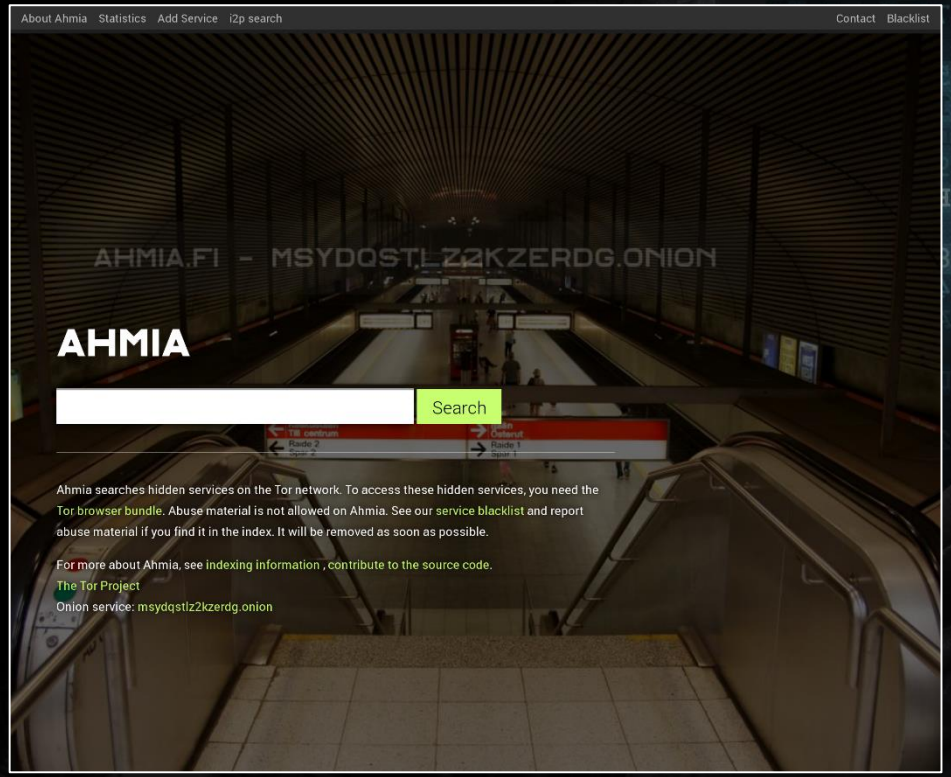
The Hidden Wiki



Popular Hidden Services

- Ahmia
  - http://msydqstlz2kzerdg.onion/
  - Fulltext Search Engine

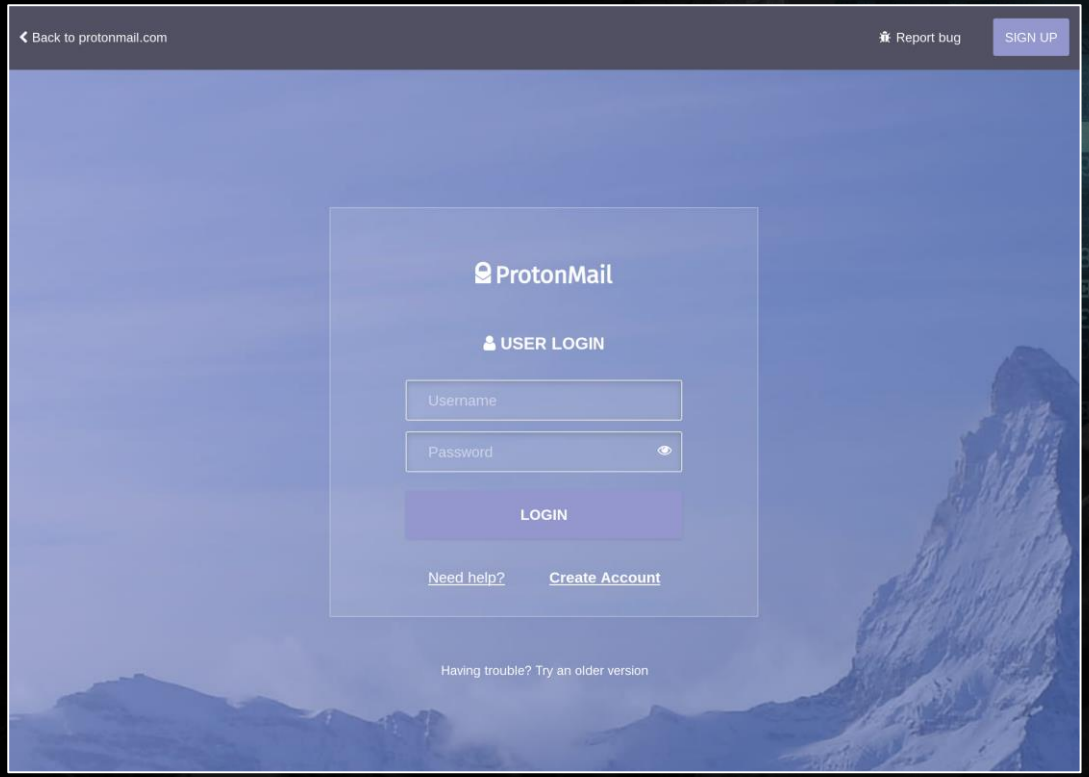
Ahmia


About Ahmia
Statistics
Add Service
i2p search
Contact
Blacklist
AHMIA.FI - MSYDQSTLZ2KZERDG.ONION
AHMIA
Search
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.
For more about Ahmia, see indexing information , contribute to the source code.
The Tor Project
Onion service: msydqstlz2kzerdg.onion

Popular Hidden Services

- ProtonMail
  - https://protonirockerxow.onion/
  - Anonymous Freemail
  - Branch of ProtonMail.com

ProtonMail


Back to protonmail.com
Report bug
SIGN UP
ProtonMail
USER LOGIN
Username
Password
LOGIN
Need help?
Create Account
Having trouble? Try an older version

Popular Hidden Services

- Daniel‘s Hosting
  - http://dhosting4okcs22v.onion/
  - Webhosting
  - Most popular webhosting at the moment
    - 4002 public hosted sites
    - 1604 hidden hosted sites
      - Deepweb
      - Let‘s hack it ☺


DEMO
Daniel‘s Hosting Real Hacking


Thank you
for your attention!
Any questions?