The Zeitgeist of Darknet

OWASP Czech Chapter Meeting
14th November 2018

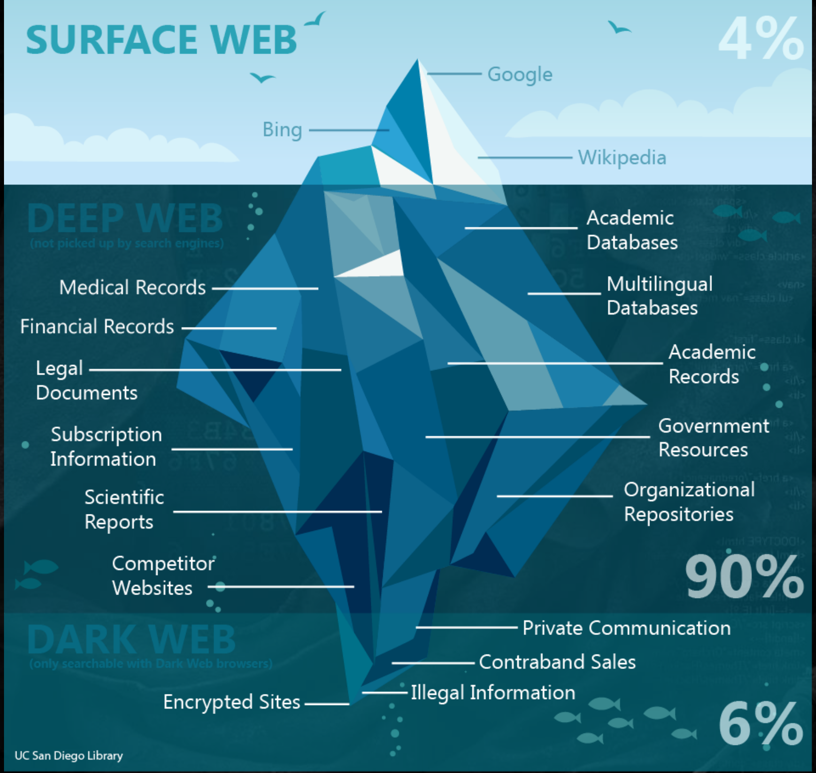
Ing. Martin Klubal
Senior IT Security Specialist
info@martinklubal.cz

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



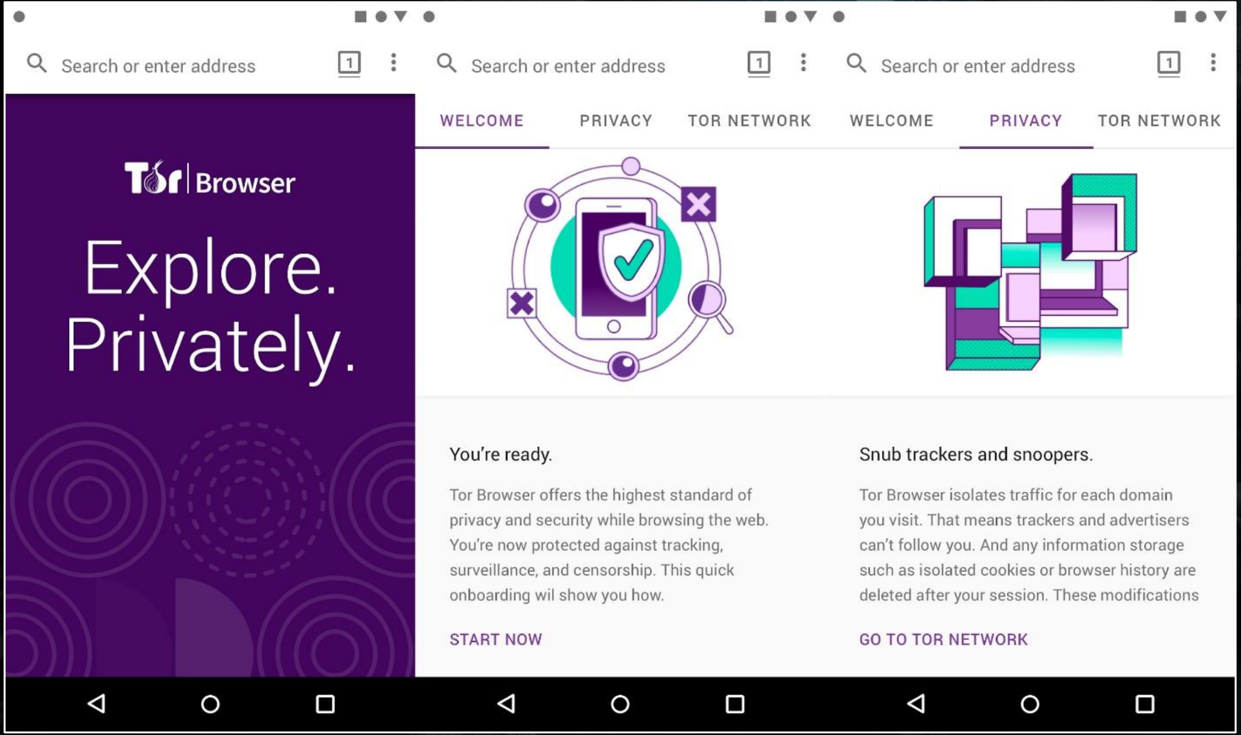
Next Gen Onion Services aka prop224

- 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)



You're ready.

Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding wil show you how.

START NOW

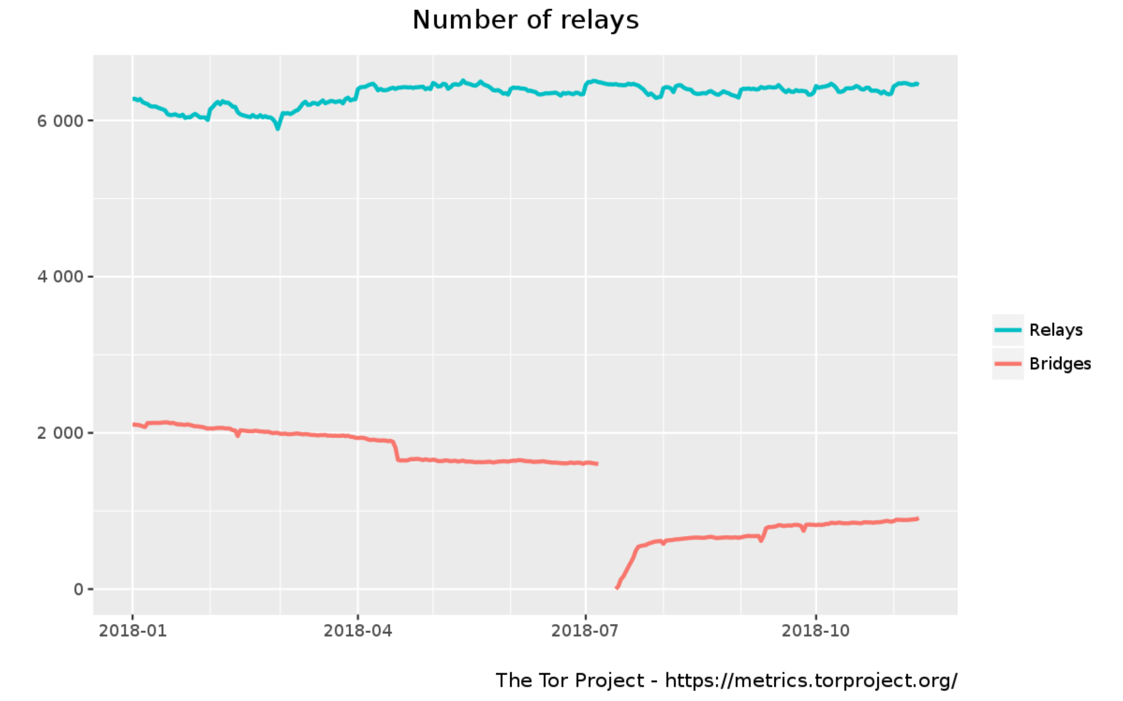
Snub trackers and snoopers.

Tor Browser isolates traffic for each domain you visit. That means trackers and advertisers can't follow you. And any information storage such as isolated cookies or browser history are deleted after your session. These modifications

GO TO TOR NETWORK

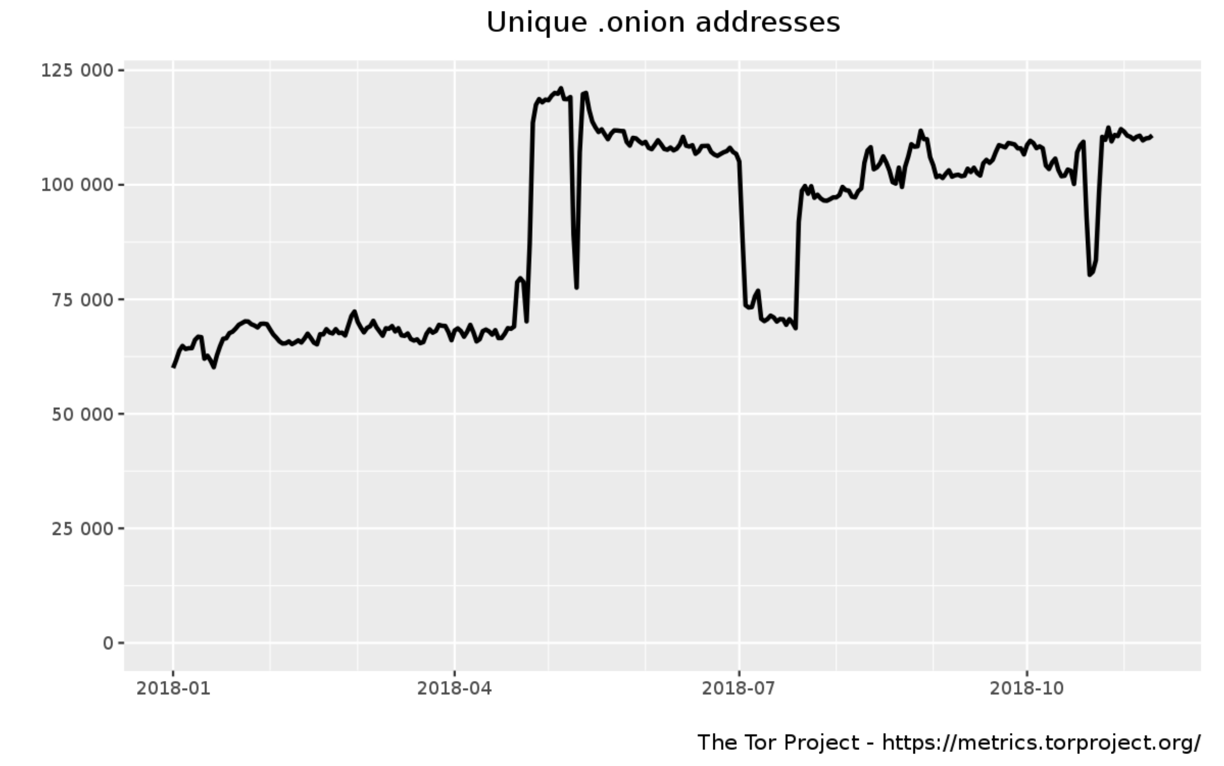
Statistics

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

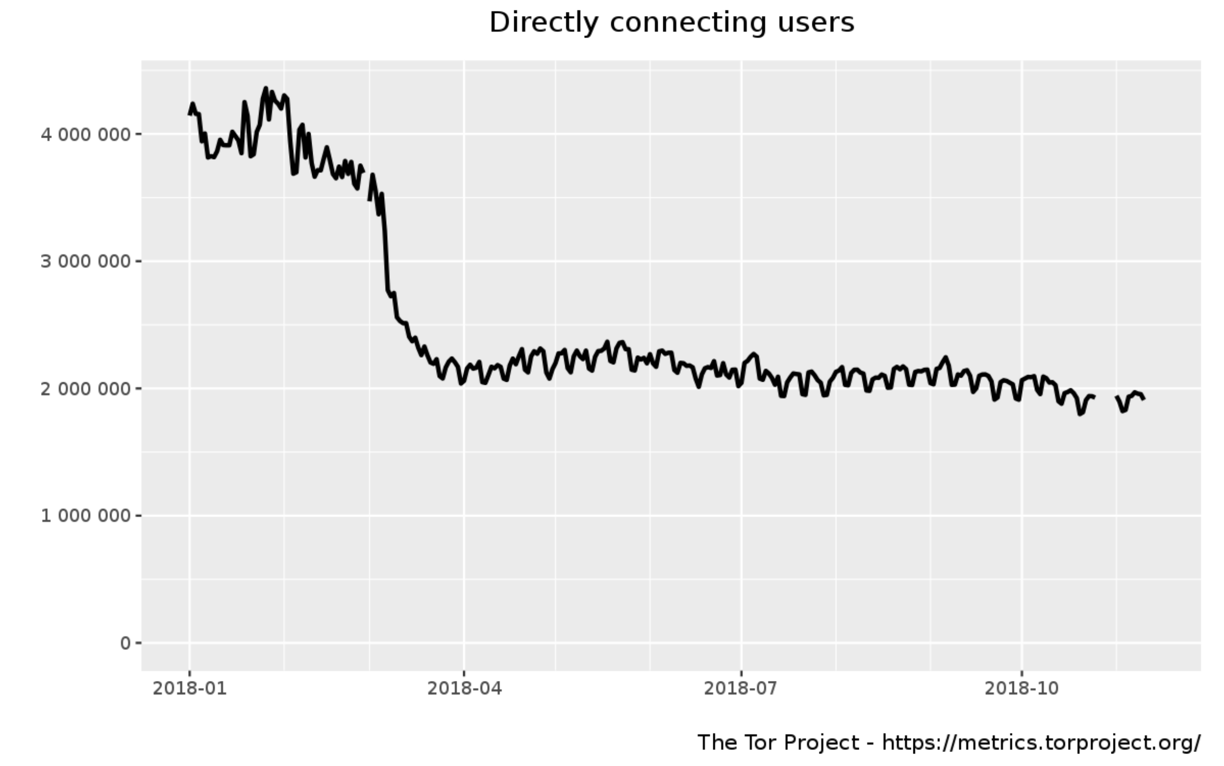


The Tor Project - https://metrics.torproject.org/

Statistics

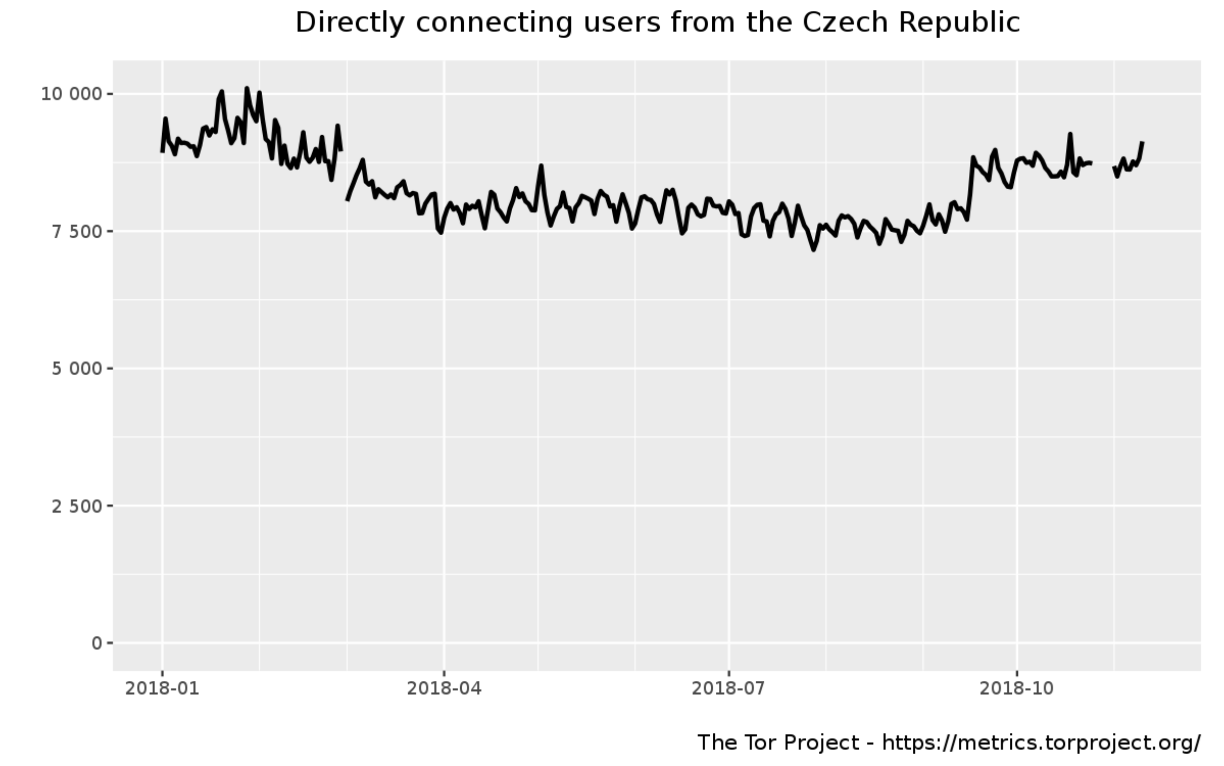

Unique .onion addresses
125 000
100 000
75 000
50 000
25 000
0
2018-01
2018-04
2018-07
2018-10
The Tor Project - https://metrics.torproject.org/

Statistics



The Tor Project - https://metrics.torproject.org/

Statistics



Directly connecting users from the Czech Republic

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

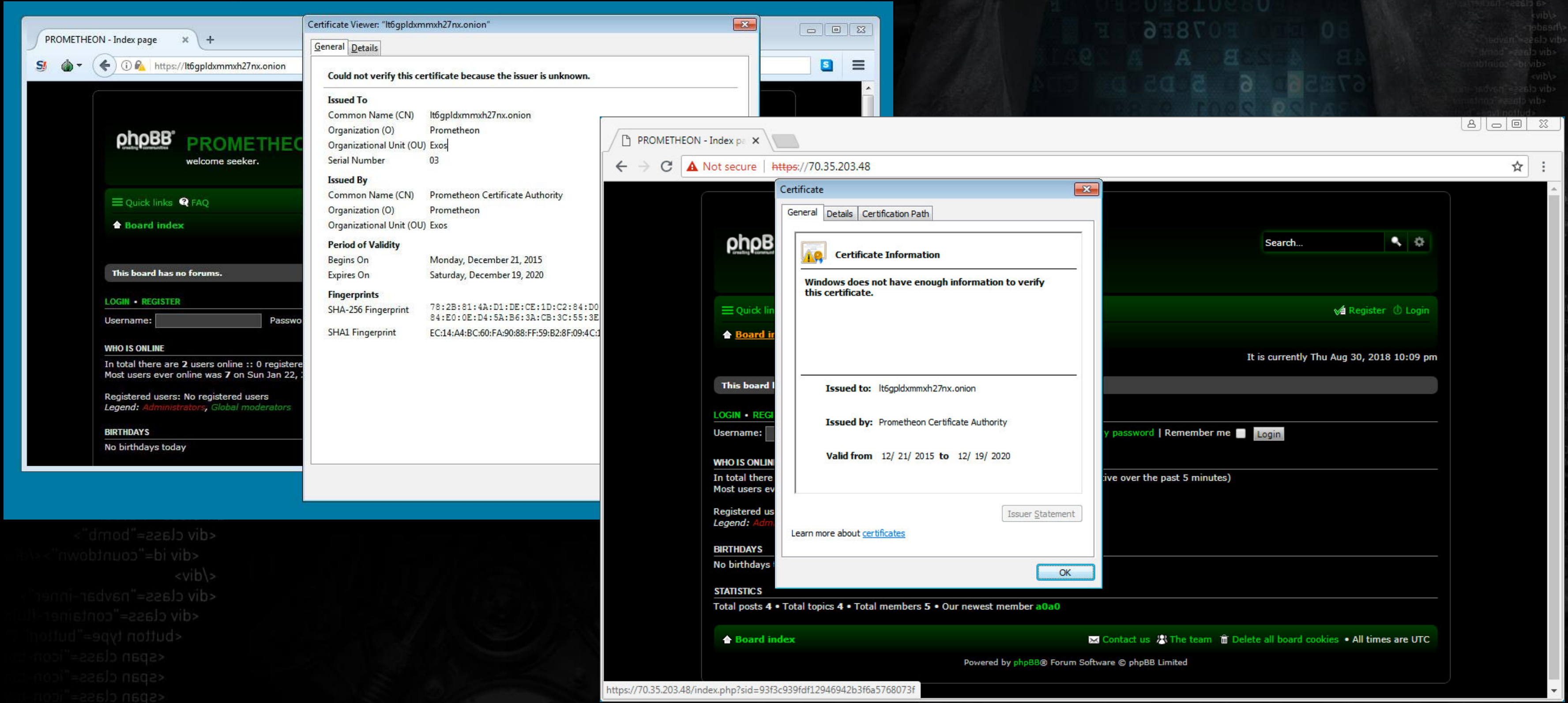
https://twitter.com/Zerodium/status/1039127214602641409

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



Certificate Viewer: "lt6gpldxmmxh27nx.onion"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	lt6gpldxmmxh27nx.onion
Organization (O)	Prometheon
Organizational Unit (OU)	Exos
Serial Number	03

Issued By

Common Name (CN)	Prometheon Certificate Authority
Organization (O)	Prometheon
Organizational Unit (OU)	Exos

Period of Validity

Begins On	Monday, December 21, 2015
Expires On	Saturday, December 19, 2020

Fingerprints

SHA-256 Fingerprint	78:2B:81:4A:D1:DE:CE:1D:C2:84:D0 84:E0:0E:D4:5A:B6:3A:CB:3C:55:3E
SHA1 Fingerprint	EC:14:A4:BC:60:FA:90:88:FF:59:B2:8F:09:4C:1

PROMETHEON - Index page — https://lt6gpldxmmxh27nx.onion

PROMETHEON - Index pa — Not secure | https://70.35.203.48

Certificate

Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: lt6gpldxmmxh27nx.onion

Issued by: Prometheon Certificate Authority

Valid from 12/ 21/ 2015 **to** 12/ 19/ 2020

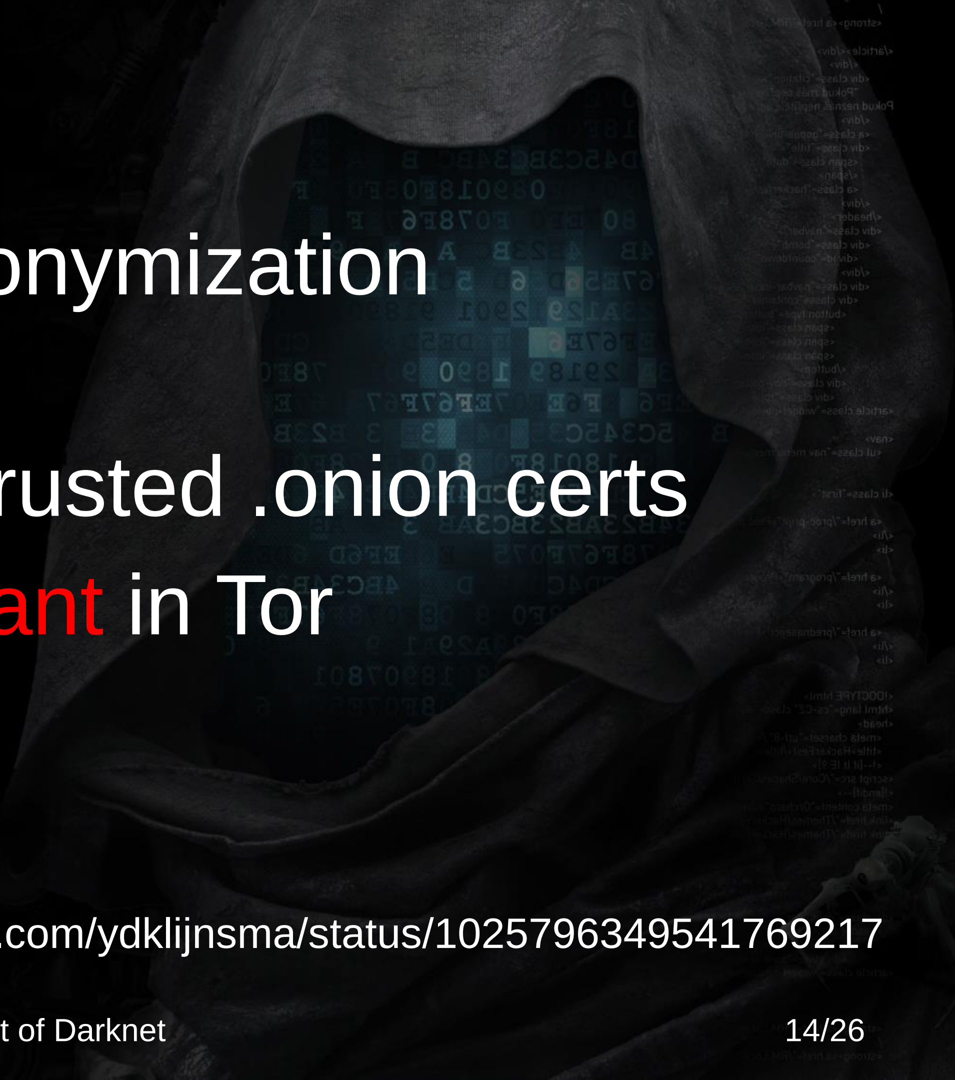
Learn more about certificates

It is currently Thu Aug 30, 2018 10:09 pm

Total posts 4 • Total topics 4 • Total members 5 • Our newest member a0a0

https://70.35.203.48/index.php?sid=93f3c939fdf12946942b3f6a5768073f

Vulnerabilities

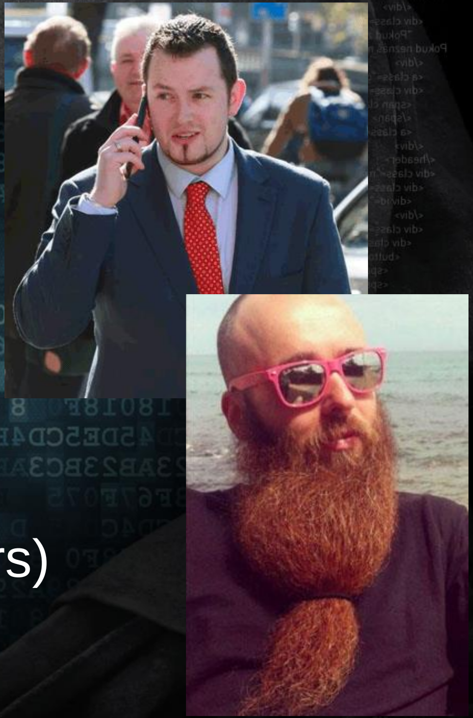


- SSL Certificate Deanonymization
  - – Use Shodan
- DigiCert.com issues trusted .onion certs
- SSL certs are redundant in Tor

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

Seizure & Conviction

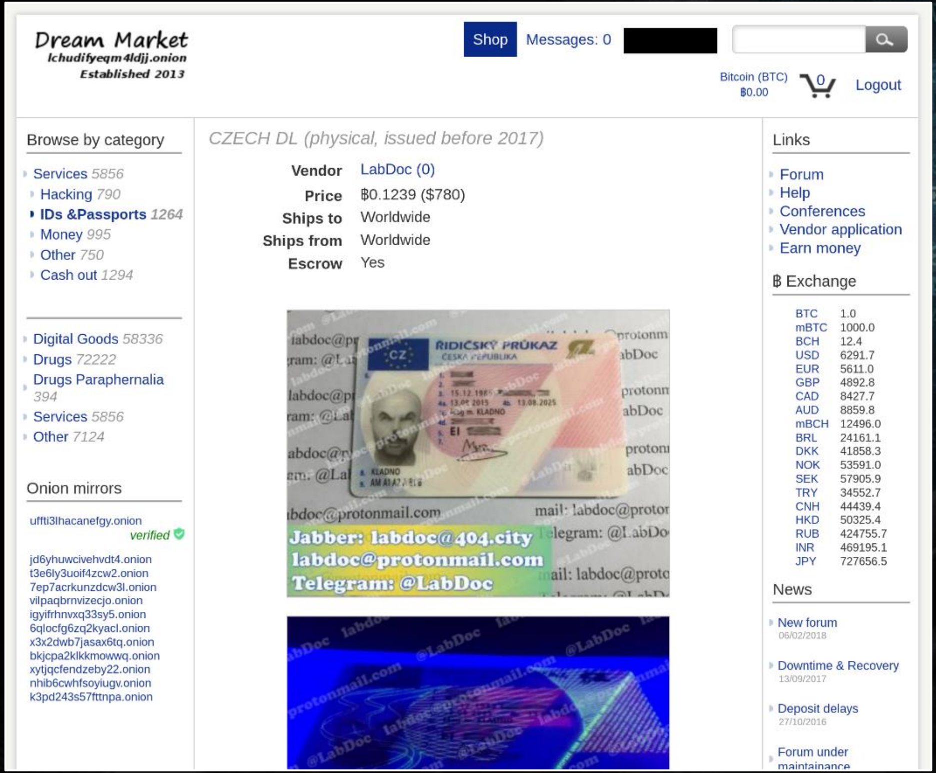
- No significant Hidden Service seized
- Conviction
  - Gary Davis (Irish)
    - Silk Road admin
    - Pleaded guilty to drug trafficking (up to 20 years)
  - Gal Vallerius (French)
    - Dream Market admin
    - Pleaded guilty to drug trafficking/launder money (20 years)



Popular Hidden Services

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

Dream Market



Dream Market
lchudifyeqm4ldjj.onion
Established 2013

Shop | Messages: 0 | [redacted]

Bitcoin (BTC)
฿0.00

0

Logout

Browse by category

- Services 5856
- Hacking 790
- **IDs &Passports 1264**
- Money 995
- Other 750
- Cash out 1294

- Digital Goods 58336
- Drugs 72222
- Drugs Paraphernalia 394
- Services 5856
- Other 7124

Onion mirrors

uffti3lhacanefgy.onion
verified

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

CZECH DL (physical, issued before 2017)

Vendor	LabDoc (0)
Price	฿0.1239 ($780)
Ships to	Worldwide
Ships from	Worldwide
Escrow	Yes

Links

- Forum
- Help
- Conferences
- Vendor application
- Earn money

฿ Exchange

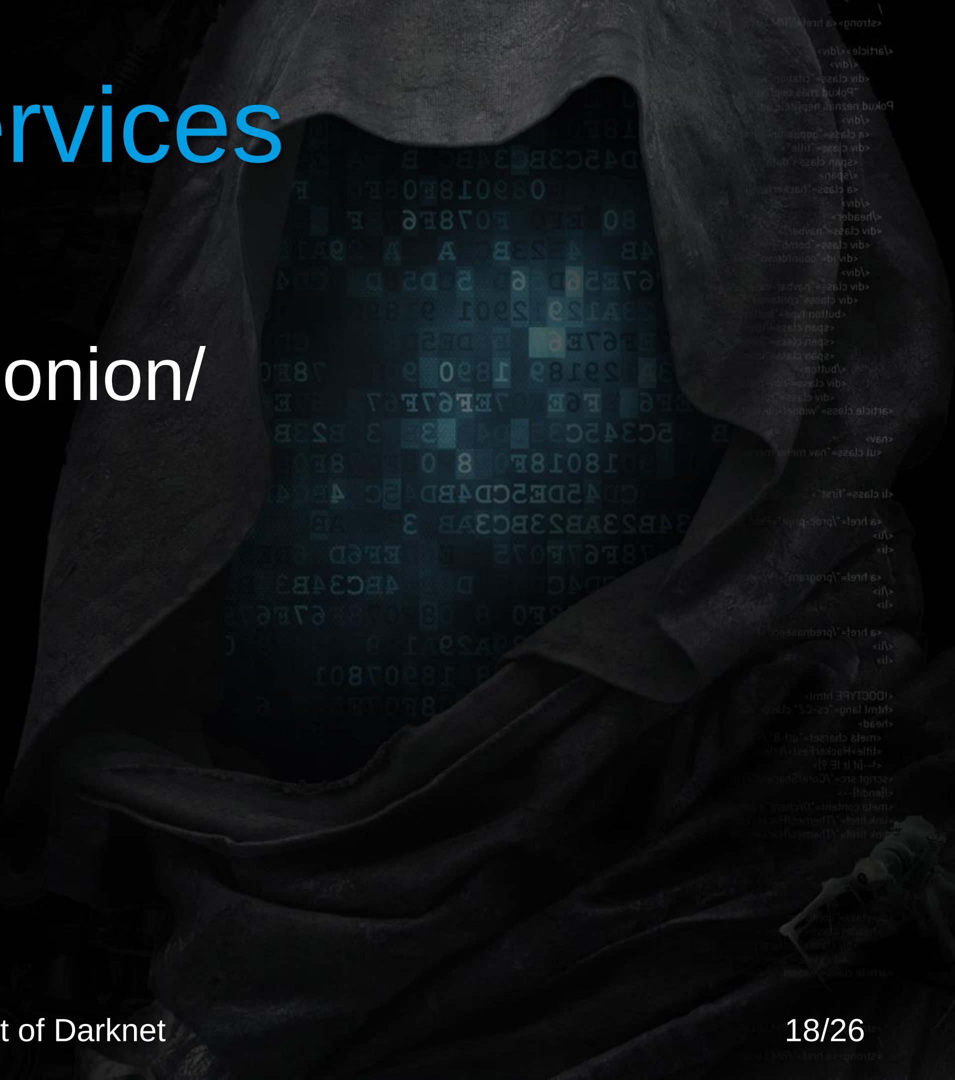
BTC	1.0
mBTC	1000.0
BCH	12.4
USD	6291.7
EUR	5611.0
GBP	4892.8
CAD	8427.7
AUD	8859.8
mBCH	12496.0
BRL	24161.1
DKK	41858.3
NOK	53591.0
SEK	57905.9
TRY	34552.7
CNH	44439.4
HKD	50325.4
RUB	424755.7
INR	469195.1
JPY	727656.5

News

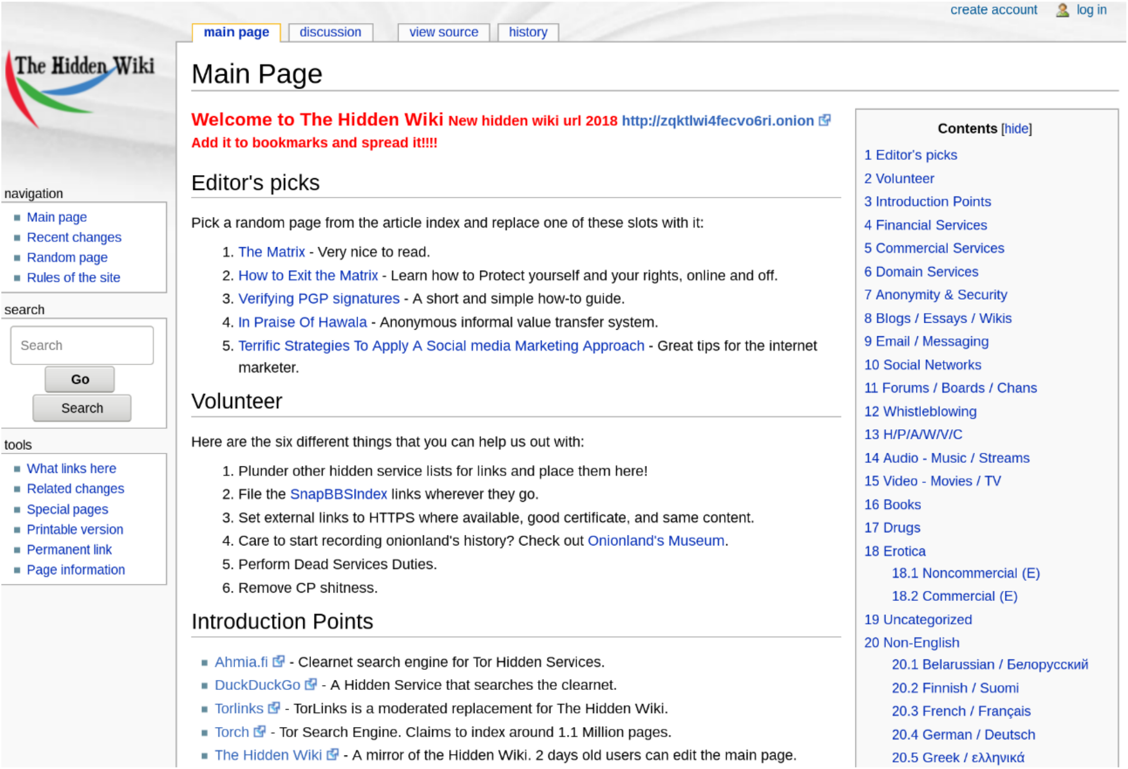
- New forum
  06/02/2018
- Downtime & Recovery
  13/09/2017
- Deposit delays
  27/10/2016
- Forum under maintainance

Popular Hidden Services

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



The Hidden Wiki



navigation

- Main page
- Recent changes
- Random page
- Rules of the site

search

Search

Go

Search

tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Main Page

Welcome to The Hidden Wiki **New hidden wiki url 2018** http://zqktlwi4fecvo6ri.onion
Add it to bookmarks and spread it!!!!

Editor's picks

Pick a random page from the article index and replace one of these slots with it:

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.
4. In Praise Of Hawala - Anonymous informal value transfer system.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.

Volunteer

Here are the six different things that you can help us out with:

1. Plunder other hidden service lists for links and place them here!
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum.
5. Perform Dead Services Duties.
6. Remove CP shitness.

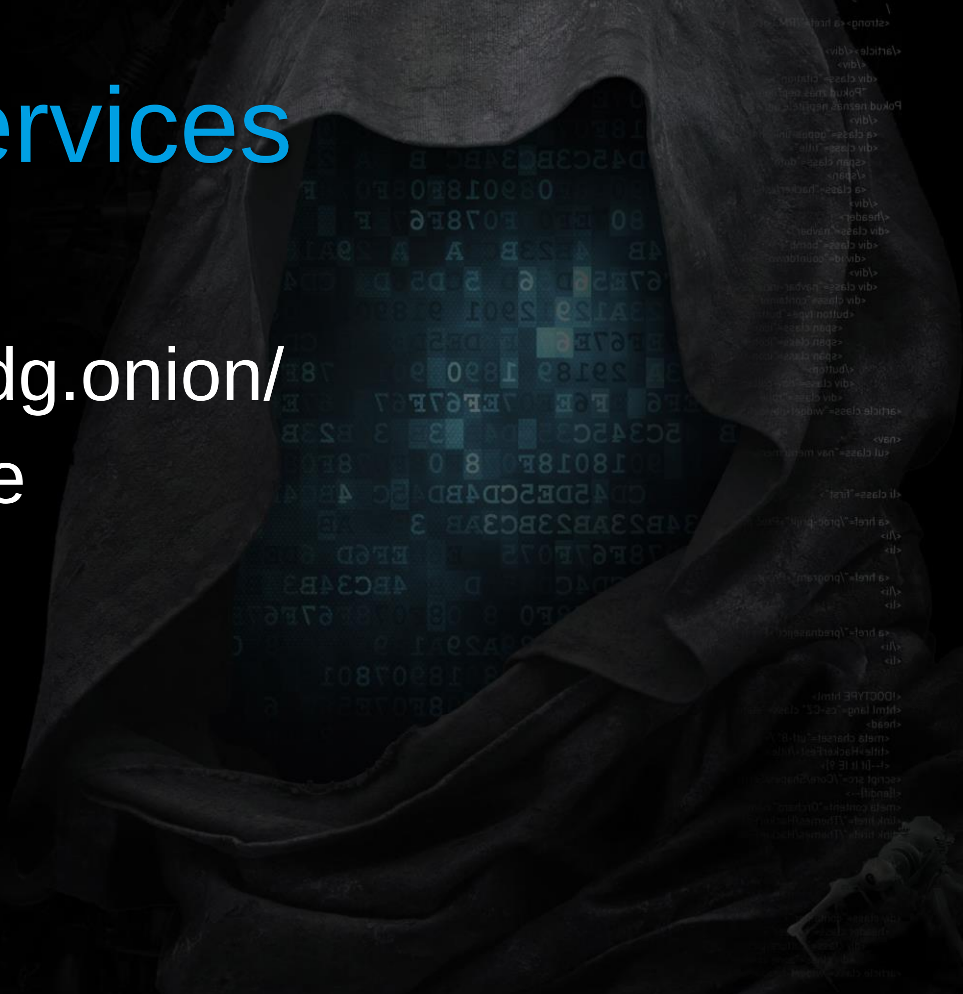
Introduction Points

- Ahmia.fi - Clearnet search engine for Tor Hidden Services.
- DuckDuckGo - A Hidden Service that searches the clearnet.
- Torlinks - TorLinks is a moderated replacement for The Hidden Wiki.
- Torch - Tor Search Engine. Claims to index around 1.1 Million pages.
- The Hidden Wiki - A mirror of the Hidden Wiki. 2 days old users can edit the main page.

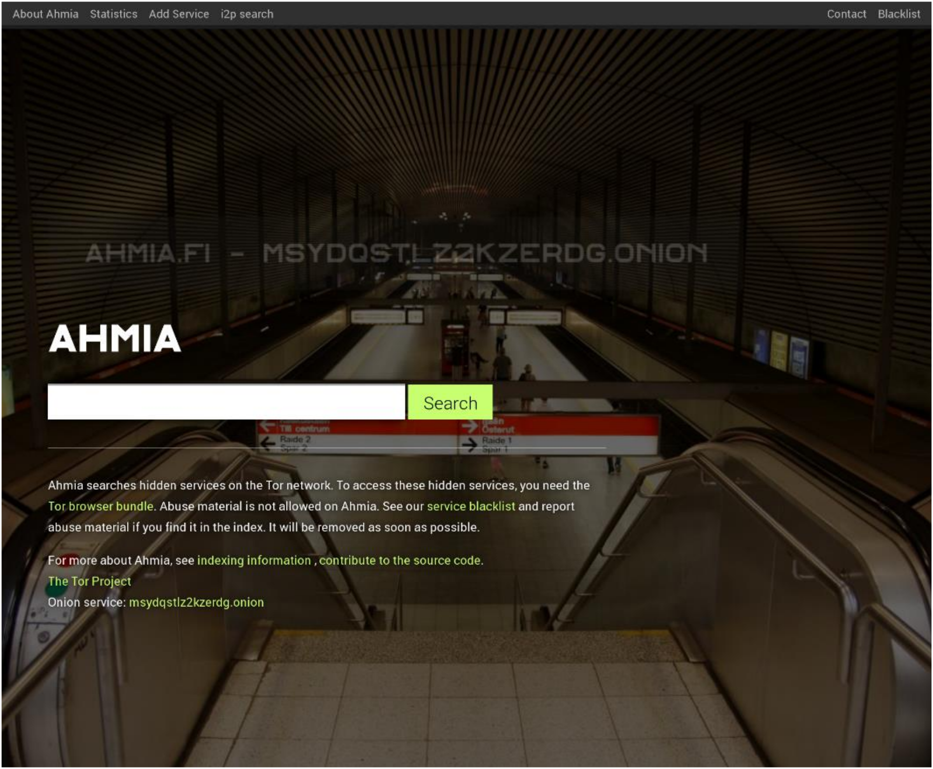
Contents [hide]

Popular Hidden Services

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



Ahmia

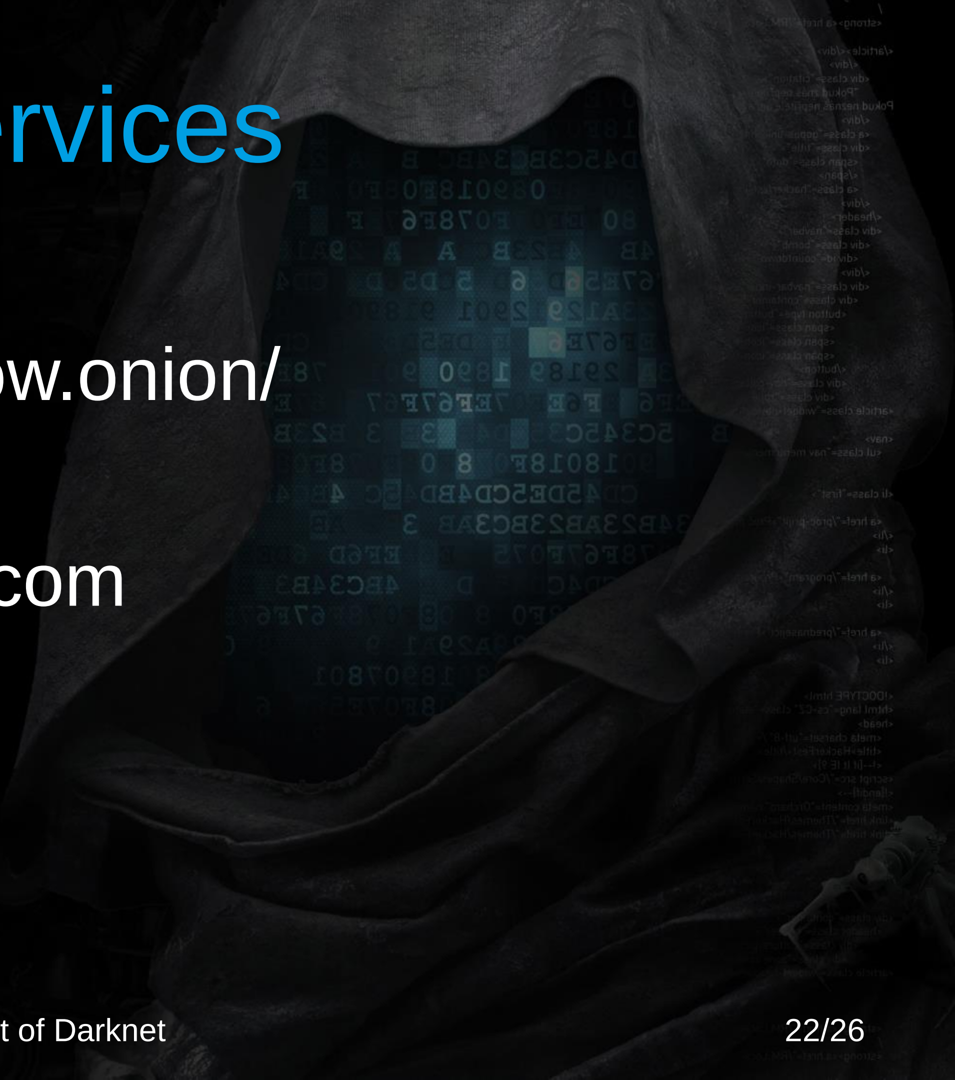


Ahmia searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.

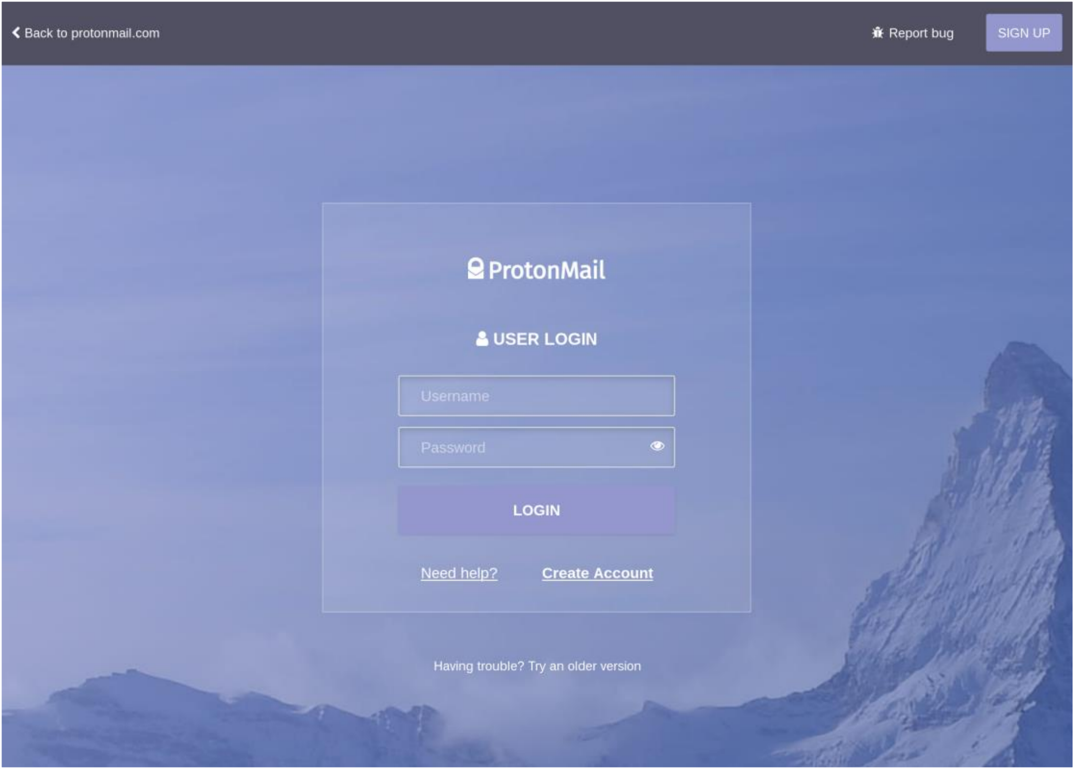
For more about Ahmia, see indexing information , contribute to the source code.
The Tor Project
Onion service: msydqstlz2kzerdg.onion

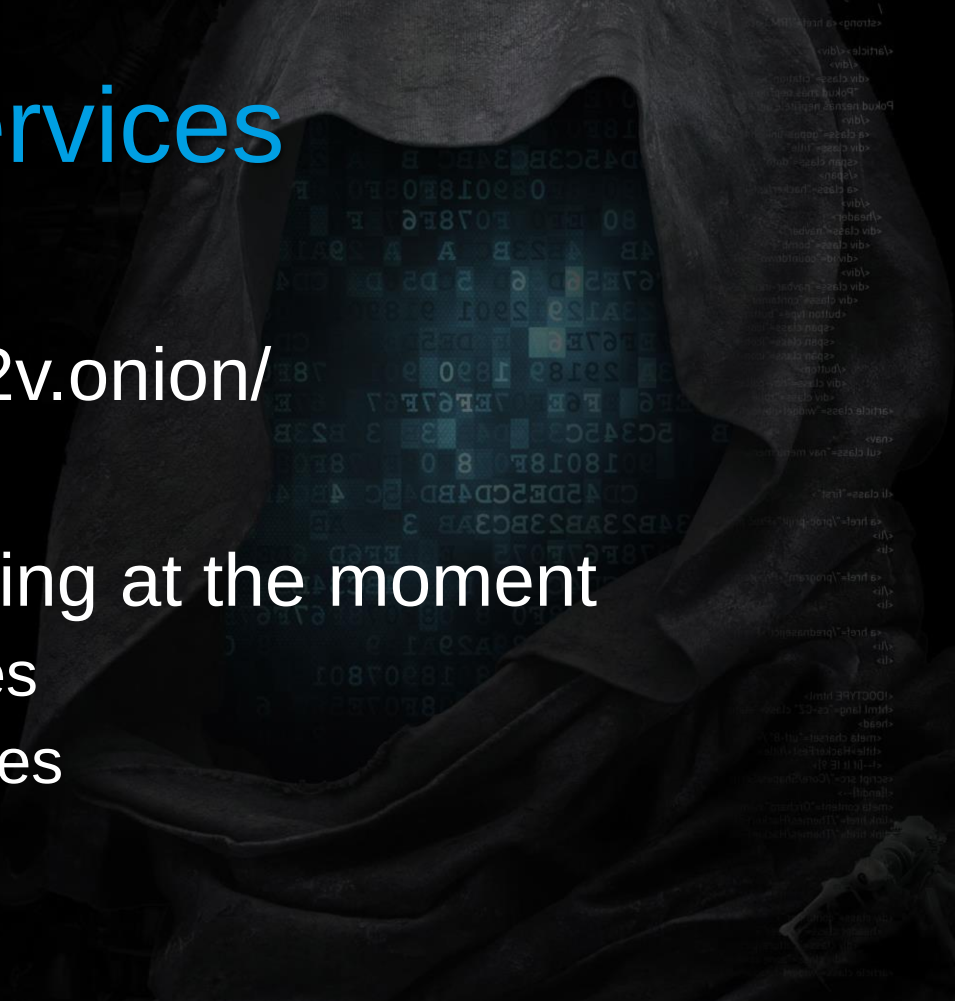
Popular Hidden Services

- 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?