

# The Zeitgeist of Darknet

OWASP Czech Chapter Meeting  
14<sup>th</sup> November 2018

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



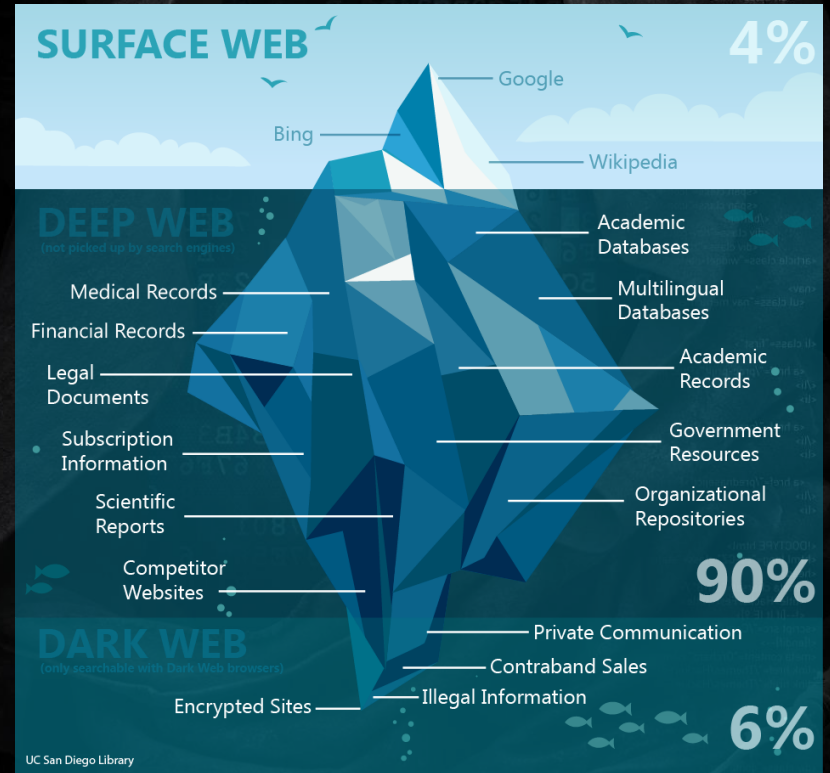
# Content

- 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

[www6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcofnpyyd.onion](http://www6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcofnpyyd.onion)



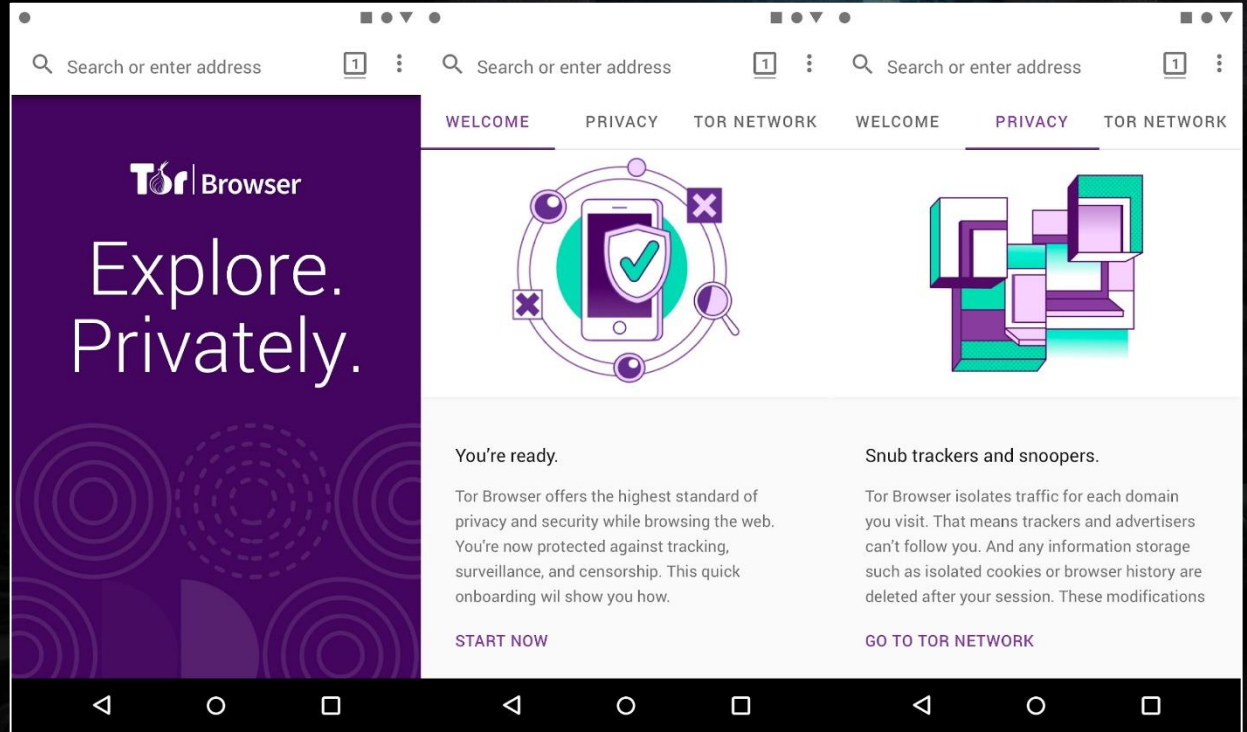
# Tor Browser for Android

- Google Play (Alpha)

[https://play.google.com/store/apps/details?id=org.torproject.torbrowser\\_alpha](https://play.google.com/store/apps/details?id=org.torproject.torbrowser_alpha)

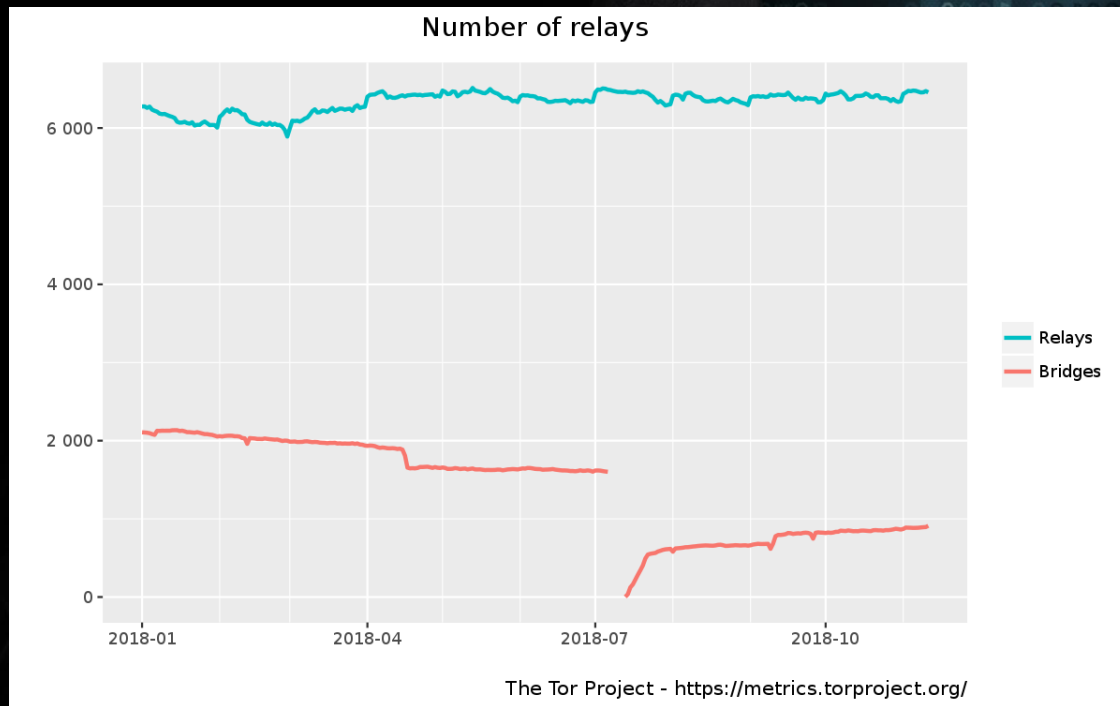
- Alternatives

- Orfox (don't use anymore)
- Onion Browser (iOS)

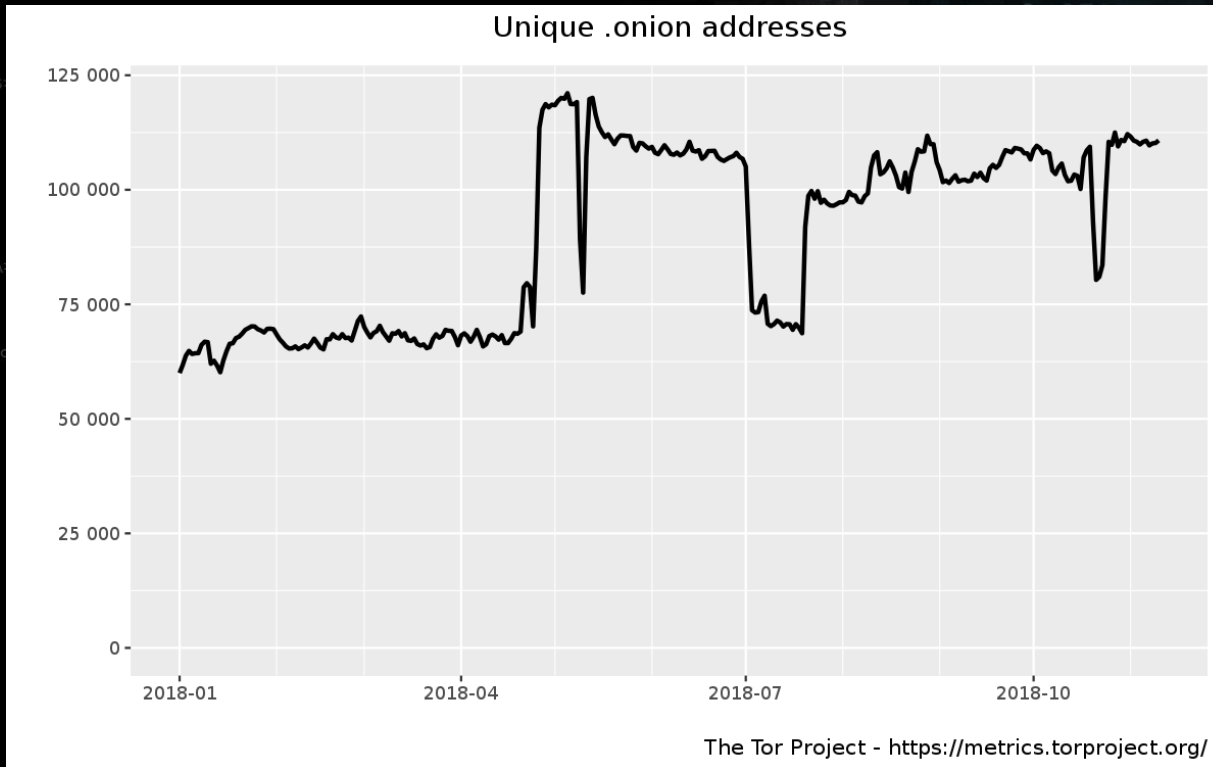


# Statistics

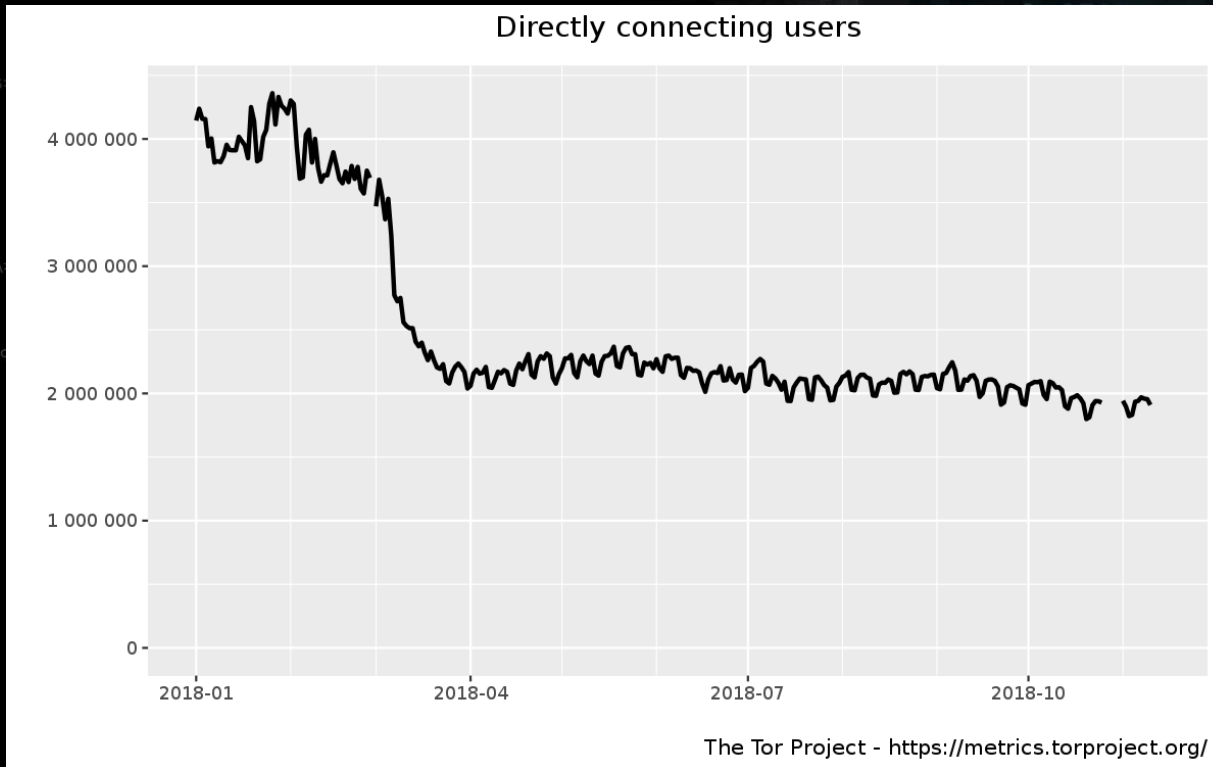
- Atlas – List of relays
  - <https://atlas.torproject.org/>



# Statistics

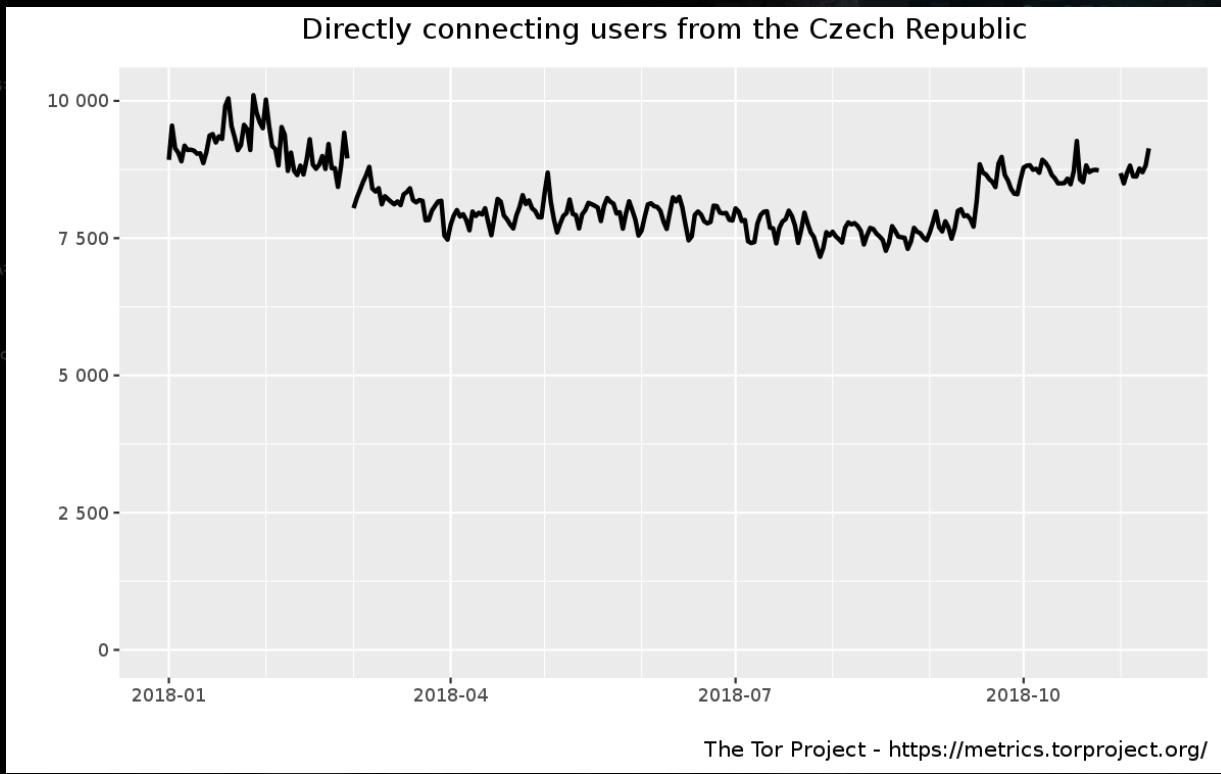


# Statistics





# Statistics



# 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 Vanguard Add-On
  - not a part of the Tor core yet

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



# SSL Certificate Deanononymization

The screenshot displays a web browser window with a security warning for an SSL certificate. The warning dialog box is open, showing the following details:

- General** | Details
- Could not verify this certificate because the issuer is unknown.
- Issued To**
  - Common Name (CN) It6gpldxmnh27rx.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:C2:84:1D084:E0:0E:D4:5A:B6:3A:CB:3C:55:3E
  - SHA1 Fingerprint EC14:A4:BC:60:FA:90:88:FF:59:B2:8F:09:4C3

The background shows the phpBB forum index page with a search bar, navigation links, and a login/register section. The browser address bar shows a "Not secure" warning for the URL <https://70.35.203.48>.



# Vulnerabilities

- SSL Certificate Deanonimization
  - 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/laundry money (20 years)



# Popular Hidden Services

- Dream Market

- <http://uffti3lhacaneffy.onion/>

- Black Market

- online from November 2013






# Popular Hidden Services


- The Hidden Wiki
  - <http://zqkltwi4fecvo6ri.onion/>
  - Directory of Links




# The Hidden Wiki

create account  log in

[main page](#) [discussion](#) [view source](#) [history](#)



## Main Page

**Welcome to The Hidden Wiki** **New hidden wiki url 2018** <http://zqkltwi4fecvo6ri.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]

- 1 Editor's picks
- 2 Volunteer
- 3 Introduction Points
- 4 Financial Services
- 5 Commercial Services
- 6 Domain Services
- 7 Anonymity & Security
- 8 Blogs / Essays / Wikis
- 9 Email / Messaging
- 10 Social Networks
- 11 Forums / Boards / Chans
- 12 Whistleblowing
- 13 H/P/AW/V/C
- 14 Audio - Music / Streams
- 15 Video - Movies / TV
- 16 Books
- 17 Drugs
- 18 Erotica
  - 18.1 Noncommercial (E)
  - 18.2 Commercial (E)
- 19 Uncategorized
- 20 Non-English
  - 20.1 Belarussian / Беларусский
  - 20.2 Finnish / Suomi
  - 20.3 French / Français
  - 20.4 German / Deutsch
  - 20.5 Greek / ελληνικά

navigation

- [Main page](#)
- [Recent changes](#)
- [Random page](#)
- [Rules of the site](#)

search

tools

- [What links here](#)
- [Related changes](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)
- [Page information](#)

# Popular Hidden Services

- Ahmia

- <http://msydqstlz2kzerdg.onion/>

- Fulltext Search Engine

# Ahmia

About Ahmia Statistics Add Service i2p search Contact Blacklist

AHMIA.FI - MSYDQSTLZKZERDG.ONION

## 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: [msydstlzkzerdg.onion](https://msydstlzkzerdg.onion)

# Popular Hidden Services

- ProtonMail

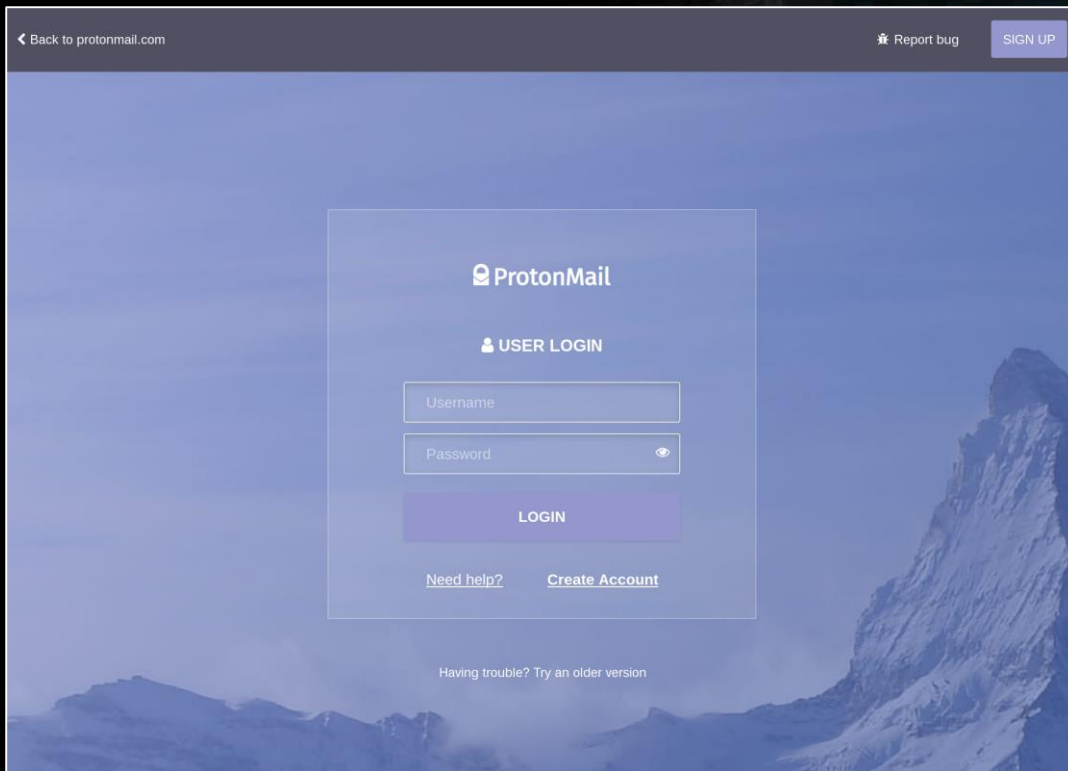
- <https://protonirockerxow.onion/>

- Anonymous Freemail

- Branch of ProtonMail.com



# ProtonMail





# 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 😊



Thank you  
for your attention!

Any questions?