The Hidden Face of the Darknet

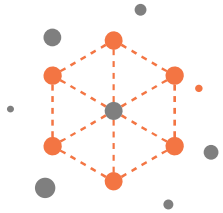
Carl Herberger
VP, Security Solutions

September 19th, 2019

Agenda

- **What is the Darknet**
- How to access the Darknet
- What can you find
- What can you buy
- Why hackers use the Darknet

What is the Darknet?



Overlay network

- Private and encrypted
- Requires specific tools

Origins

- 1970, Isolated network from ARPANET

Uses

- Email and social media
- Hosting and file sharing
- News and Media
- E-Commerce

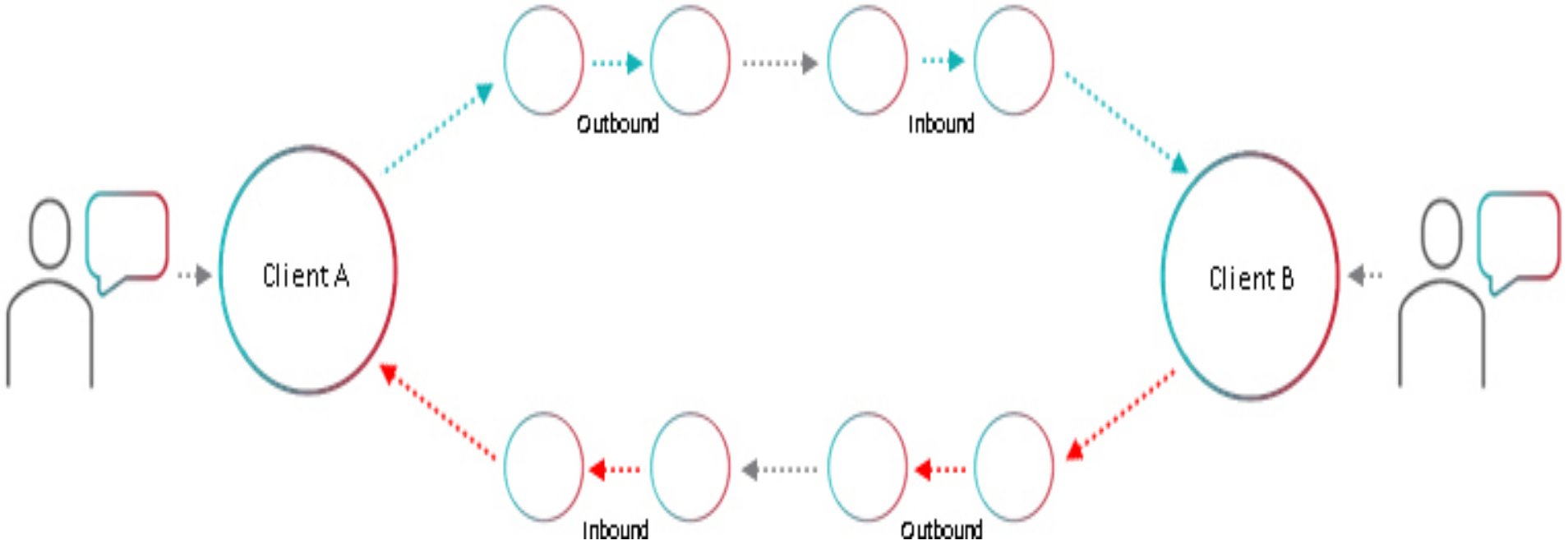
Agenda

- What is the Darknet
- **How to access the Darknet**
- What can you find
- What can you buy
- Why hackers use the Darknet

How to access the Darknet?

	TOR	I2P
Software	The Onion Router	Invisible Internet Project
Two Dark-net Types	Anonymity	Friend-to-Friend
Uses	Privacy / Hidden Services	File sharing

Type of Darknet – I2P



I2P ROUTER CONSOLE

HELP & FAQ
I2P SERVICES
Email Torrents Website
I2P INTERNALS
Tunnels Peers Profiles NetDB Logs
Graphs Stats Addressbook
Hidden Services Manager

GENERAL

Local Identity:	show
Version:	0.9.26-0
Uptime:	26 sec

Network: OK

Restart Shutdown

PEERS

Active:	5 / 5
Fast:	0
High capacity:	150
Integrated:	190
Known:	279

BANDWIDTH IN/OUT

3 sec:	0.54 / 1.49 KBps
Used:	5.94 KB / 23.62 KB

TUNNELS

9/27/16: Congratulations On Getting I2P Installed!

Welcome to I2P! Please **have patience** as I2P boots up and finds peers.

While you are waiting, please **adjust your bandwidth settings** on the **configuration page**.

Also you can setup your browser to use the I2P proxy to reach eepsites. Just enter 127.0.0.1 (or localhost) port 4444 as a http proxy into your browser settings. Do not use SOCKS for this. More information can be found on the **I2P browser proxy setup page**.

Once you have a "shared clients" destination listed on the left, please **check out** our **FAQ**.

Point your IRC client to **localhost:6668** and say hi to us on **#i2p**.

Welcome to I2P

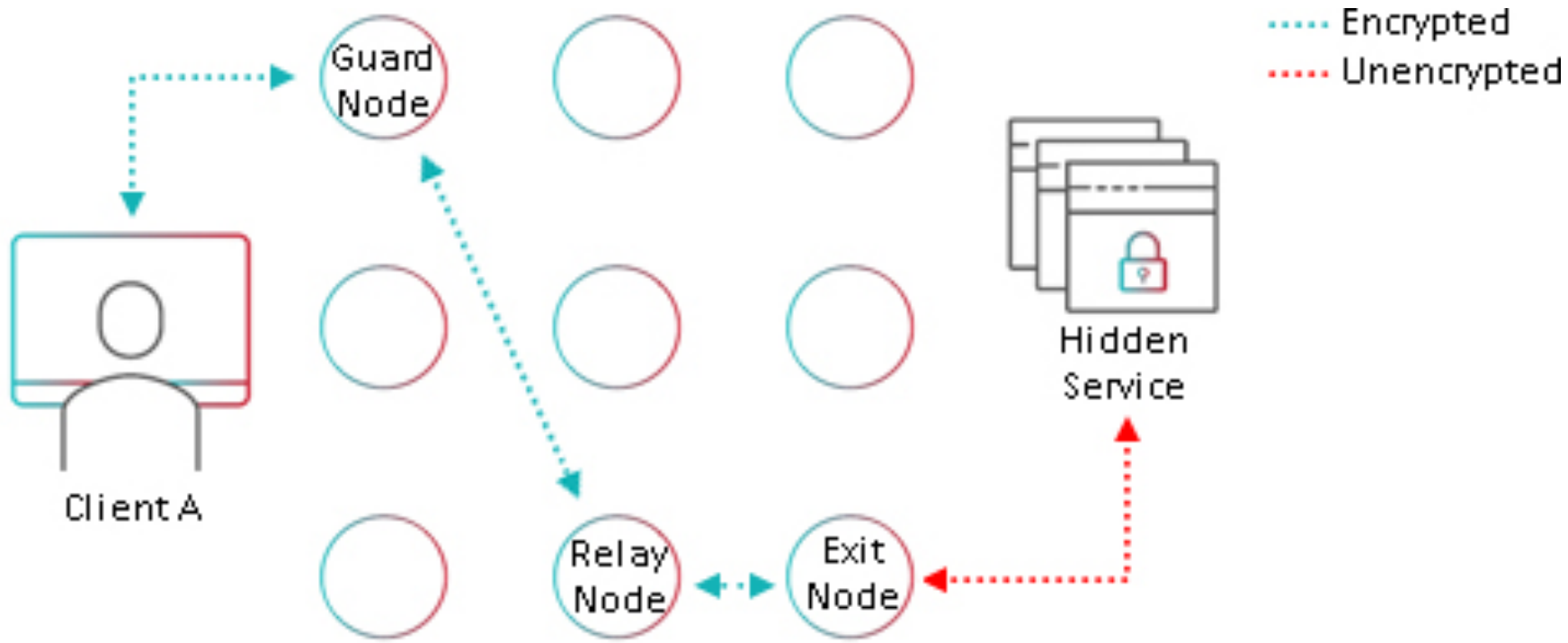
Starting Up...

If you've just started I2P, the number of *Active Peers* indicated under the *Peers* section in the side panel on the left should start to grow over the next few minutes and you'll also see a *Local Destination* named *Shared Clients* listed there, and possibly other clients and servers depending on how I2P is configured (if not, see the troubleshooting section **below**). These *Local Destinations* provide connections on different ports (and sometimes protocols) to the I2P network, enabling your bittorrent, e-mail, web proxy and other services to function. Your **Network Database** indicates all known peers on the network. Additionally, you can monitor existing **Peer Connections**, and view existing **Tunnels** and their status. More information is available on the **help page**.

Network integration

The first time you start I2P it may take a few minutes to bootstrap (integrate) you into the network and find additional peers to optimize your integration, so please be patient. When I2P starts up, and during normal operation, I2P's tunnel build readiness indicator (immediately above the *Local Destinations* section in the sidepanel) may tell you that I2P is "Rejecting Tunnels"; this is normal behavior and should be of no cause for concern! Once green stars are indicated next to your *Local Destinations*, there is a wide variety of things you can do with I2P, and below we introduce you to some of them.

Type of Darknet – Tor



About Tor

Tor Browser | Search with DuckDuckGo or enter address

Search

TOR: STRENGTH IN NUMBERS

Mozilla is matching every donation until 2019.

Give now, and your gift becomes twice as strong.

Donate Now

Tor Browser is all new.
See what you can do!

Tor Browser
8.0.4

Explore. Privately.

You're ready for the world's most private browsing experience.

Search with DuckDuckGo

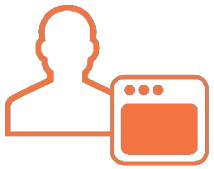
Questions? Check our Tor Browser Manual »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

Whonix

Two virtual machines

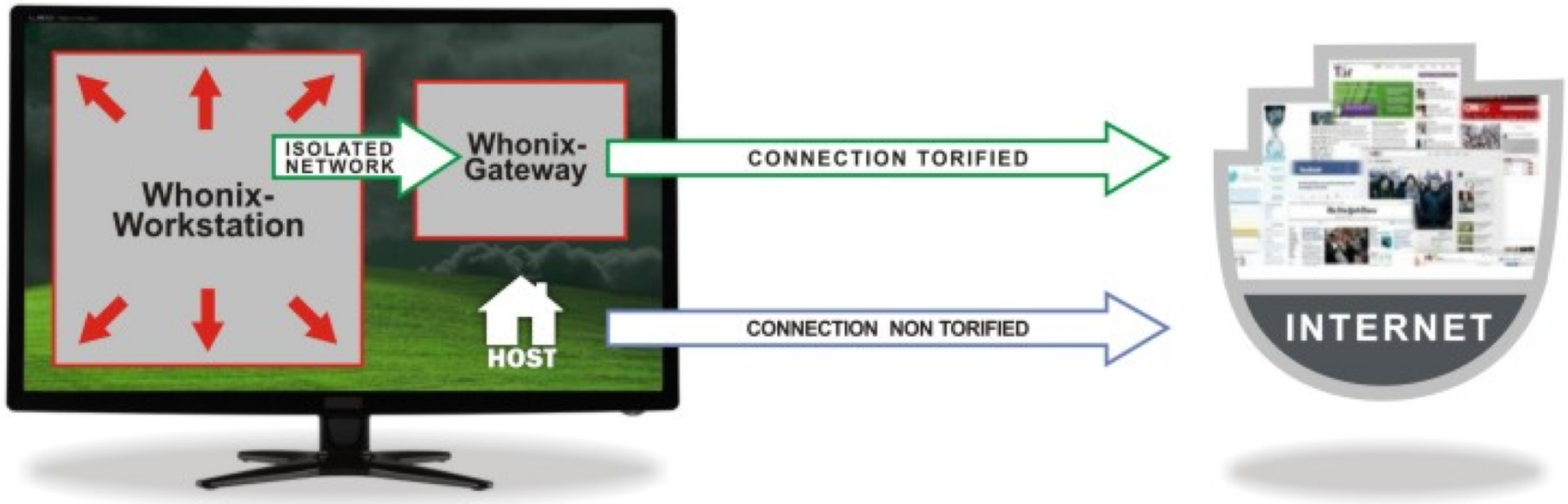
- Workstation
- Gateway



User application have no knowledge of the users ‘real’ IP address

All communications are forced through the Tor network

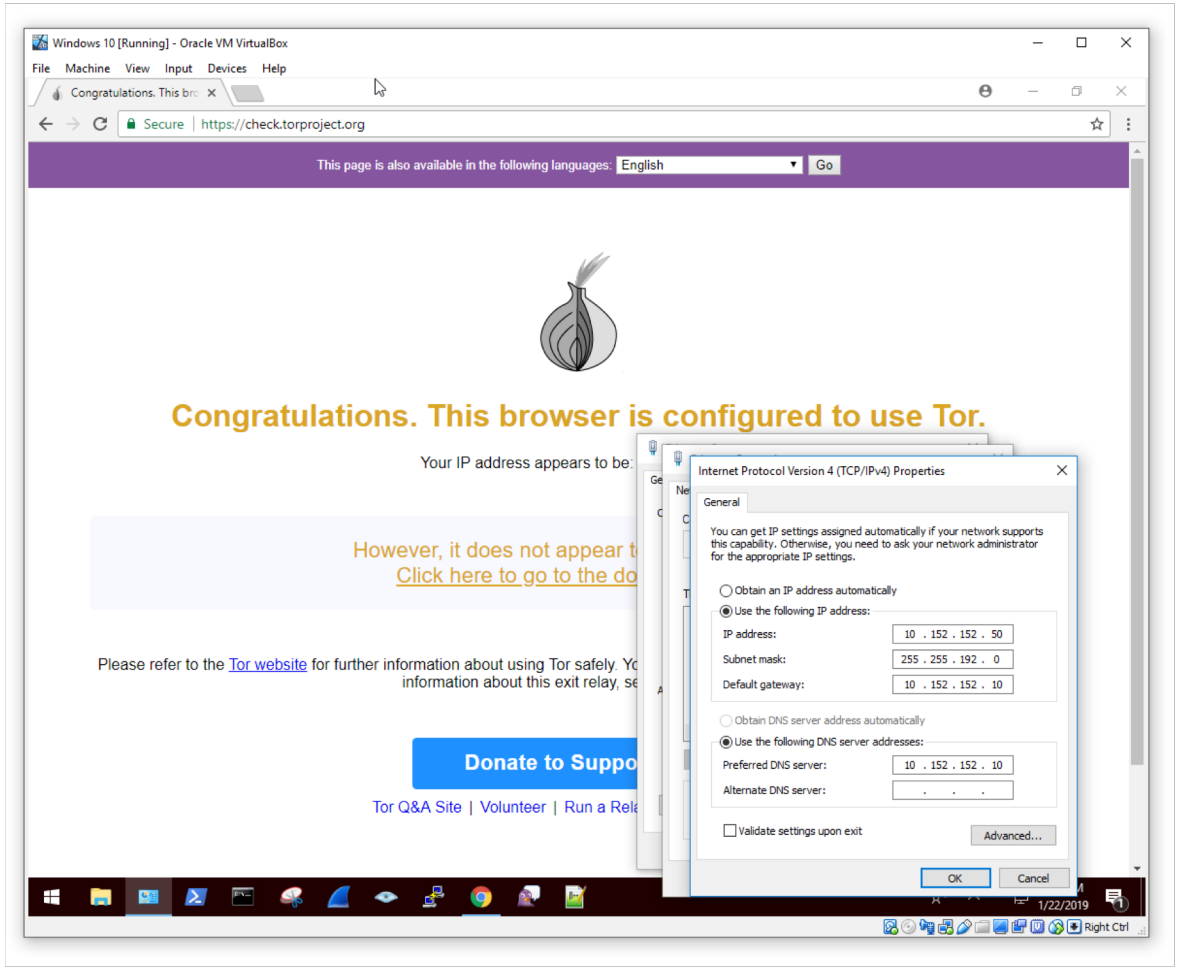
Whonix
Anonymous Operating System

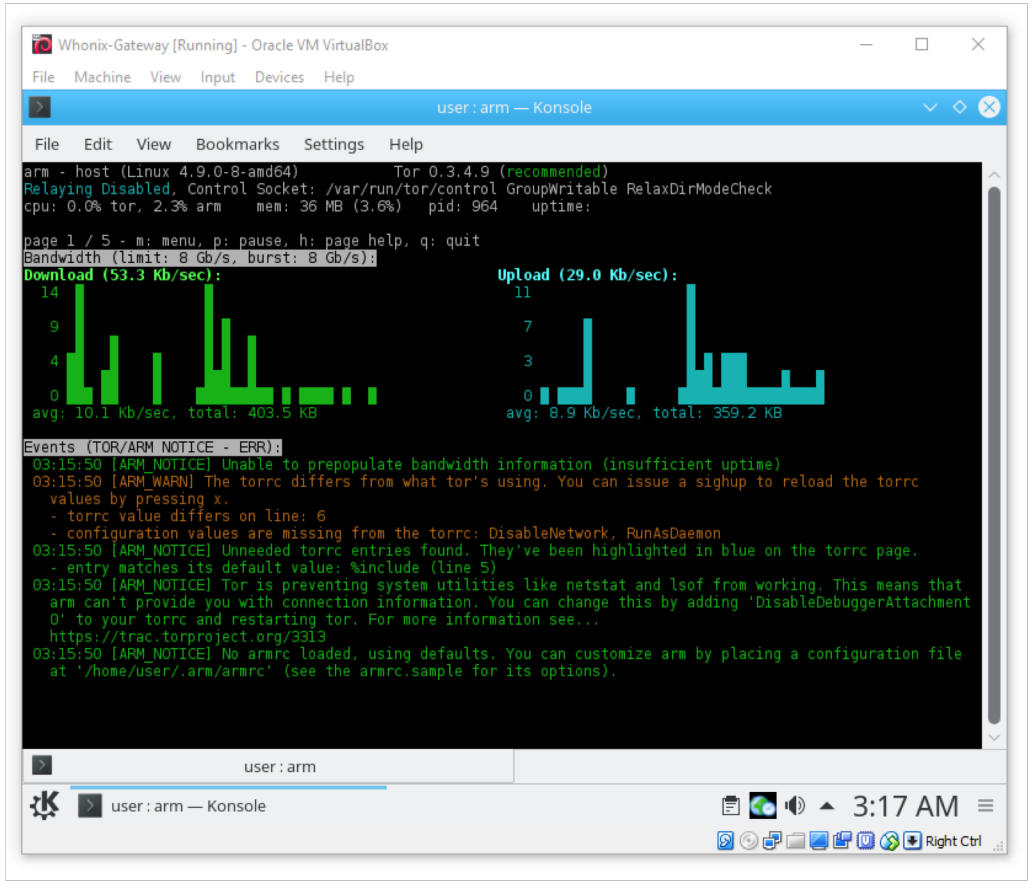


The red arow ↗ *indicate that misbehaving / leaky applications can't break out of the* **Whonix Workstation**.

All network connections ⇨ *are forced to go through* **Whonix Gateway** *where they are torified and routed to the Internet.*

Whonix

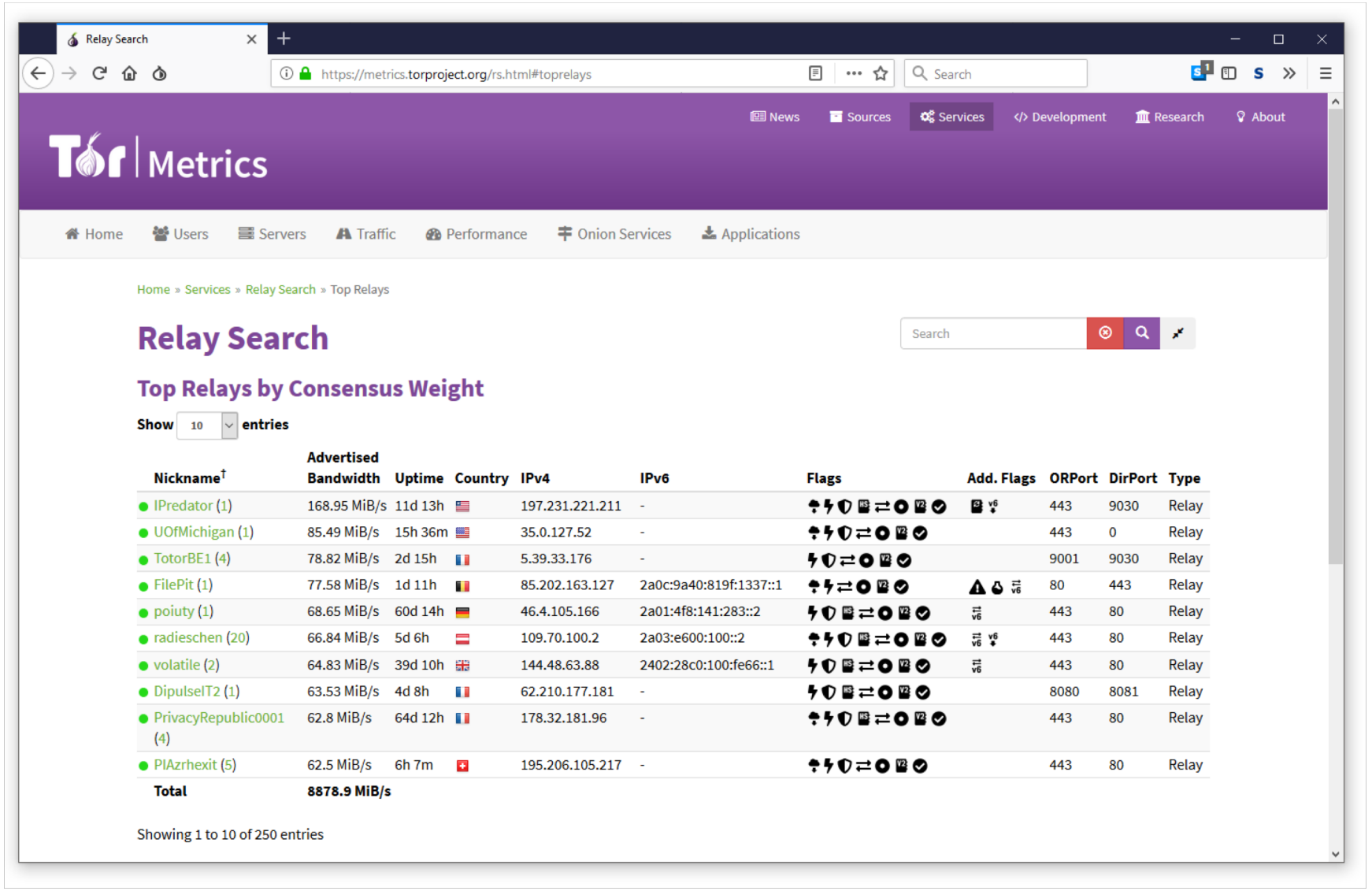

Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Congratulations. This bro
Secure | https://check.torproject.org
This page is also available in the following languages: English Go
Congratulations. This browser is configured to use Tor.
Your IP address appears to be:
However, it does not appear t
Click here to go to the do
Please refer to the Tor website for further information about using Tor safely. Yo
information about this exit relay, se
Donate to Suppo
Tor Q&A Site | Volunteer | Run a Rela
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 152 . 152 . 50
Subnet mask: 255 . 255 . 192 . 0
Default gateway: 10 . 152 . 152 . 10
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 152 . 152 . 10
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1/22/2019
Right Ctrl


Whonix-Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user : arm — Konsole
File Edit View Bookmarks Settings Help
arm - host (Linux 4.9.0-8-amd64) Tor 0.3.4.9 (recommended)
Relaying Disabled, Control Socket: /var/run/tor/control GroupWritable RelaxDirModeCheck
cpu: 0.0% tor, 2.3% arm mem: 36 MB (3.6%) pid: 964 uptime:
page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 8 Gb/s, burst: 8 Gb/s):
Download (53.3 Kb/sec):
14
9
4
0
avg: 10.1 Kb/sec, total: 403.5 KB
Upload (29.0 Kb/sec):
11
7
3
0
avg: 8.9 Kb/sec, total: 359.2 KB
Events (TOR/ARM NOTICE - ERR):
03:15:50 [ARM_NOTICE] Unable to prepopulate bandwidth information (insufficient uptime)
03:15:50 [ARM_WARN] The torrc differs from what tor's using. You can issue a sighup to reload the torrc values by pressing x.
- torrc value differs on line: 6
- configuration values are missing from the torrc: DisableNetwork, RunAsDaemon
03:15:50 [ARM_NOTICE] Unneeded torrc entries found. They've been highlighted in blue on the torrc page.
- entry matches its default value: %include (line 5)
03:15:50 [ARM_NOTICE] Tor is preventing system utilities like netstat and lsof from working. This means that arm can't provide you with connection information. You can change this by adding 'DisableDebuggerAttachment 0' to your torrc and restarting tor. For more information see...
https://trac.torproject.org/3313
03:15:50 [ARM_NOTICE] No armrc loaded, using defaults. You can customize arm by placing a configuration file at '/home/user/.arm/armrc' (see the armrc.sample for its options).
user : arm
user : arm — Konsole
3:17 AM
Right Ctrl

Agenda

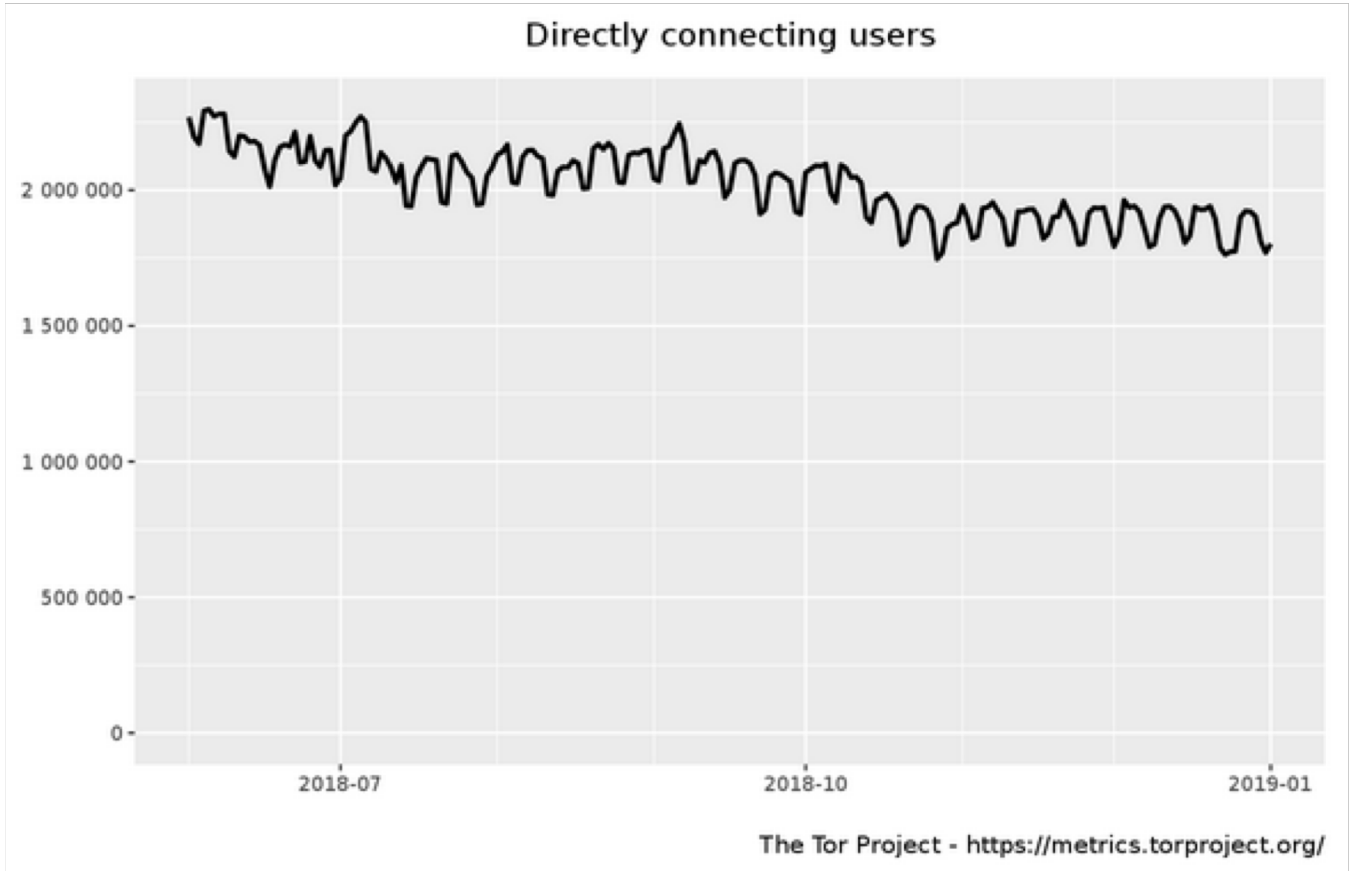
- What is the Darknet
- How to access the Darknet
- **What can you find**
- What can you buy
- Why hackers use the Darknet

Metrics – Tor Project



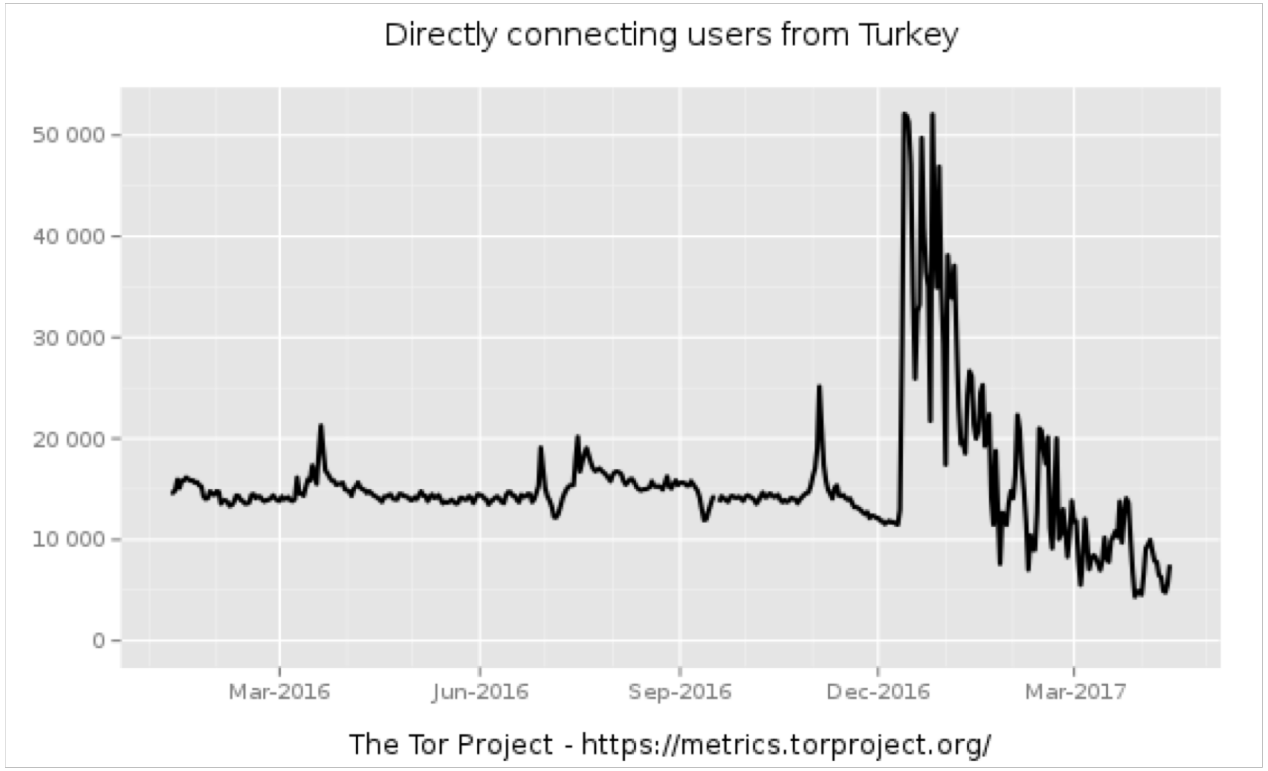
Metrics

- Around 2 Million users per day
- United States has the most daily users
- Spikes of usage show possible censorship



Censorship - Turkey

- December 2016 Turkey begins censoring the internet
- Sites like Facebook, Twitter and YouTube blocked
- Arrest over comments on the internet
- Spike in Tor relay users follow
- Tor, VPN websites blocked
- Increase in bridge users



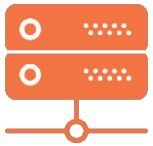
What can you find on the Darknet?

News sites

Forums

E-commerce

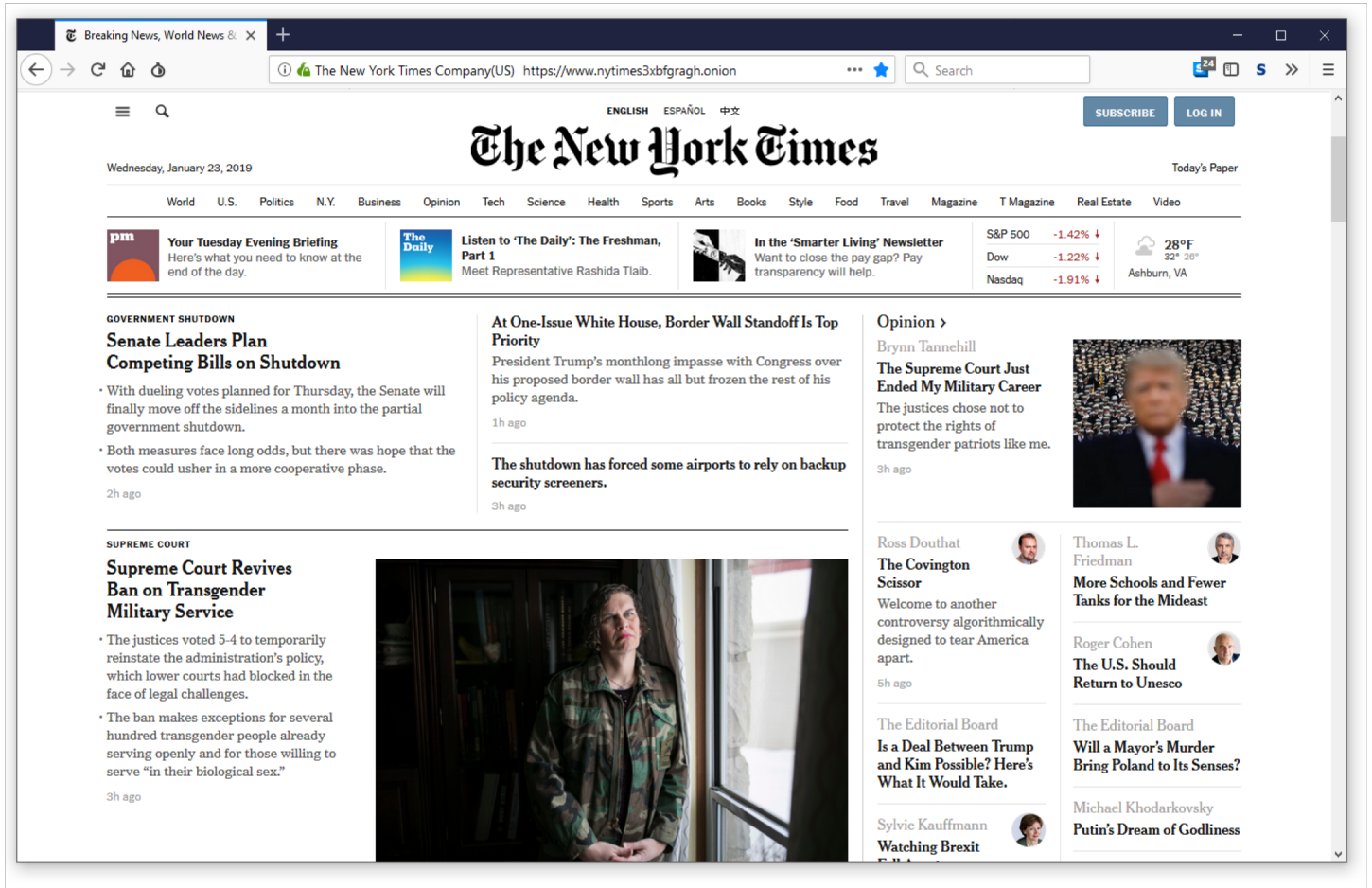
Email services



Hosting service

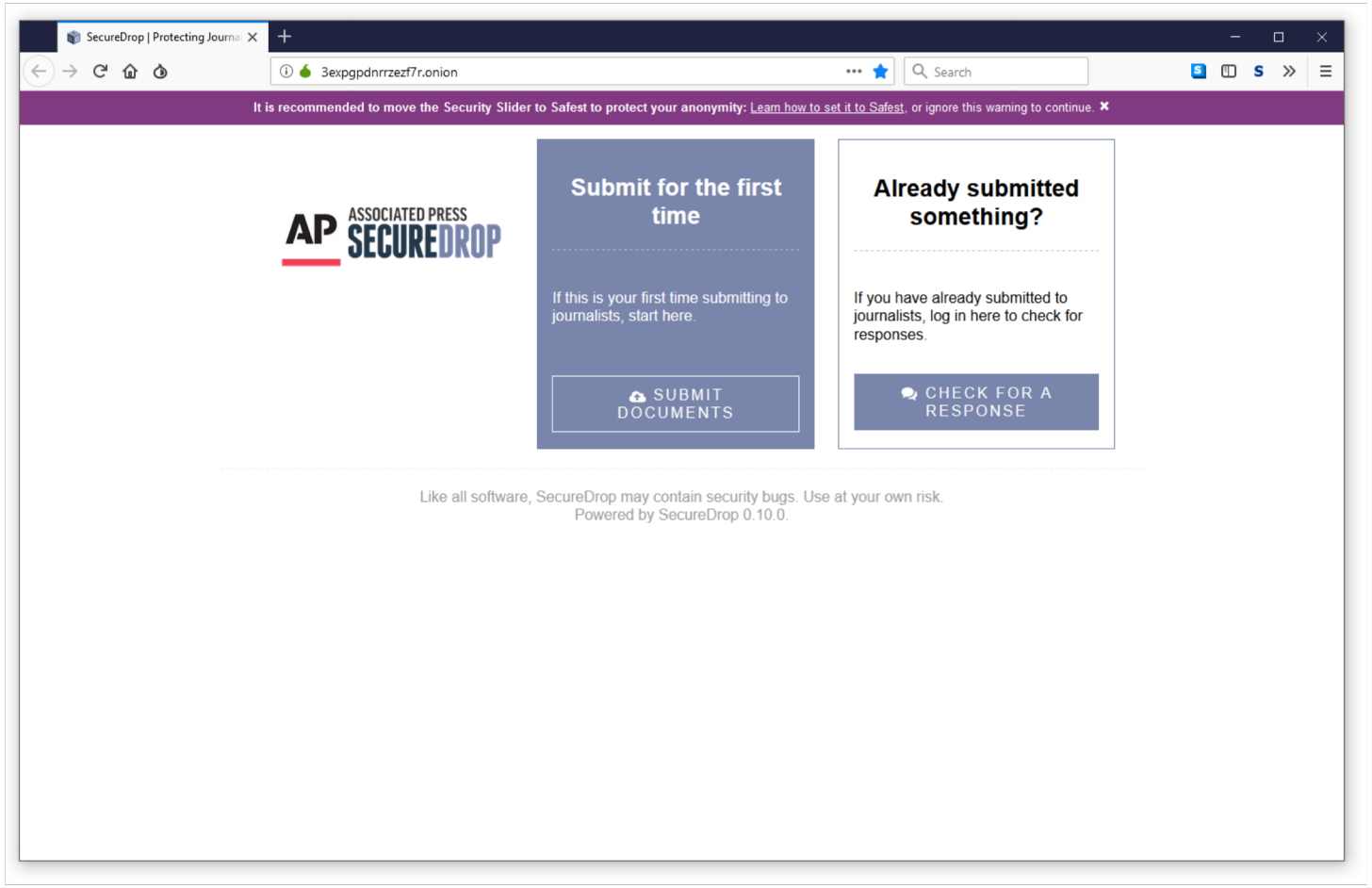
New York Times

- Mirrored news services
- Counter censorship & surveillance
- Securely submit information



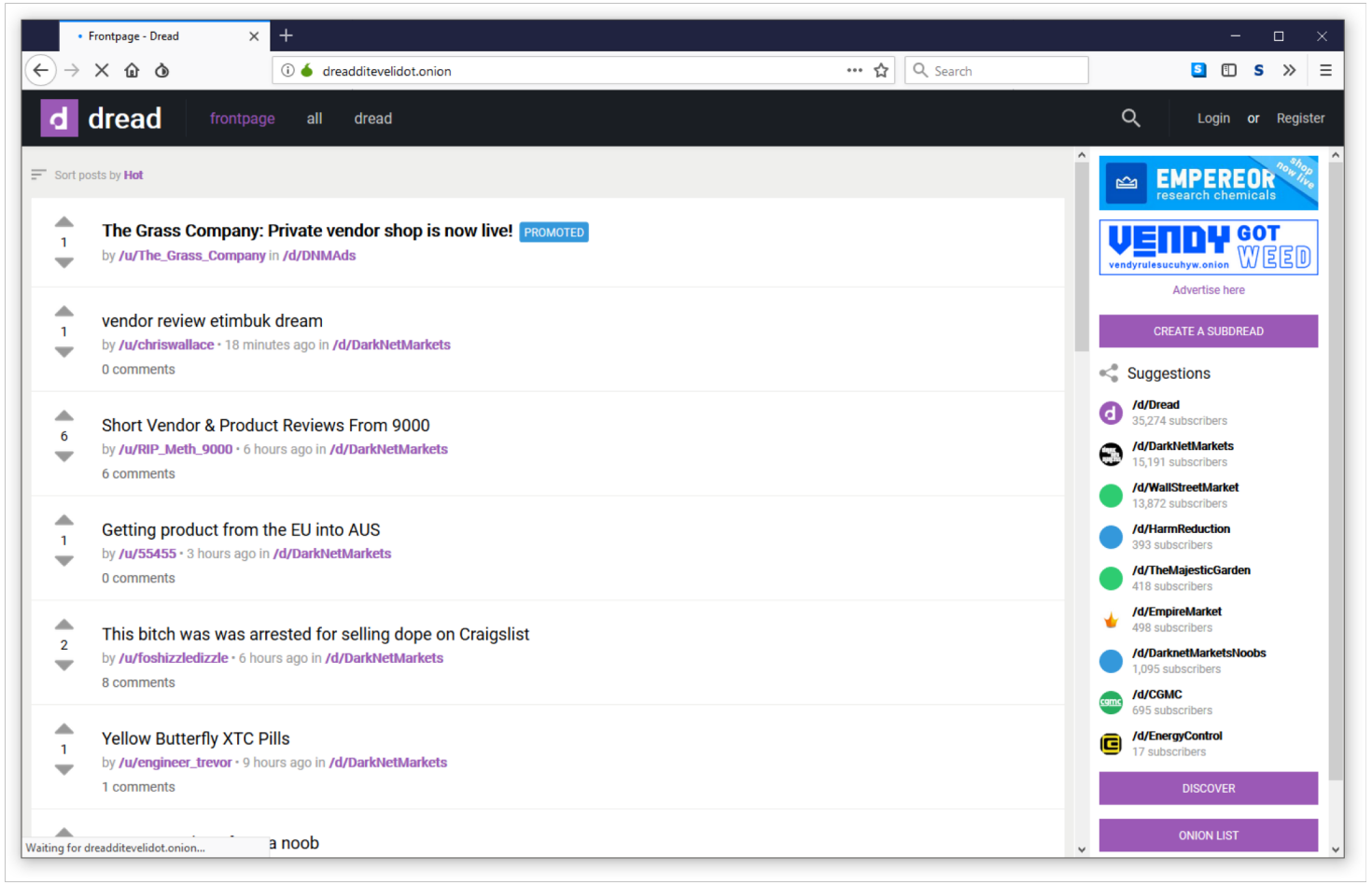
Secure Drop

- Anonymously submit tips to trusted news sources via a Hidden Service



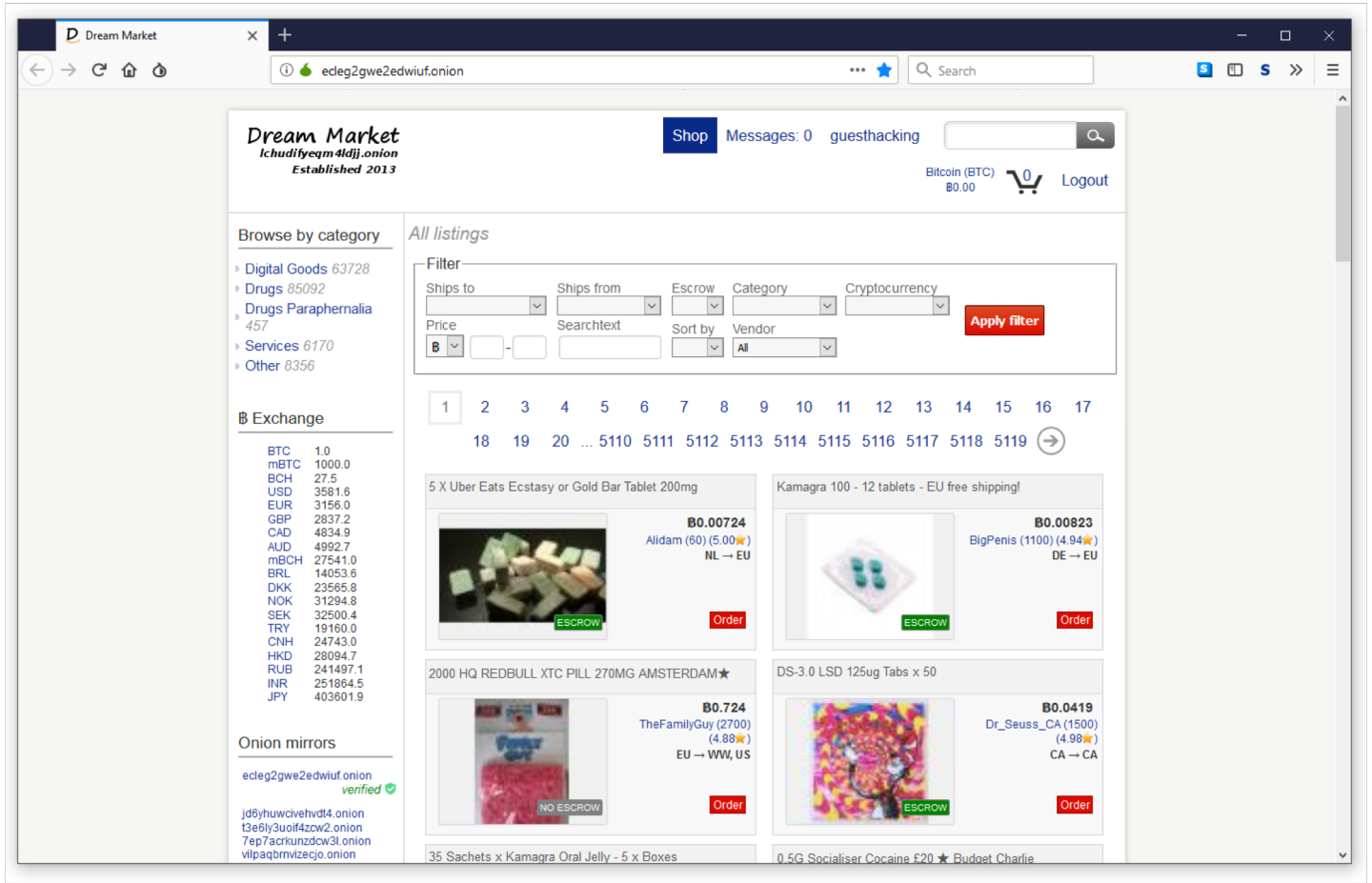
Forums

- Variety of options and languages
  - Independent forums
  - Associated with marketplaces
  - Mirrored forums
- Hacking Forums
  - Knowledge exchange
  - Marketplace

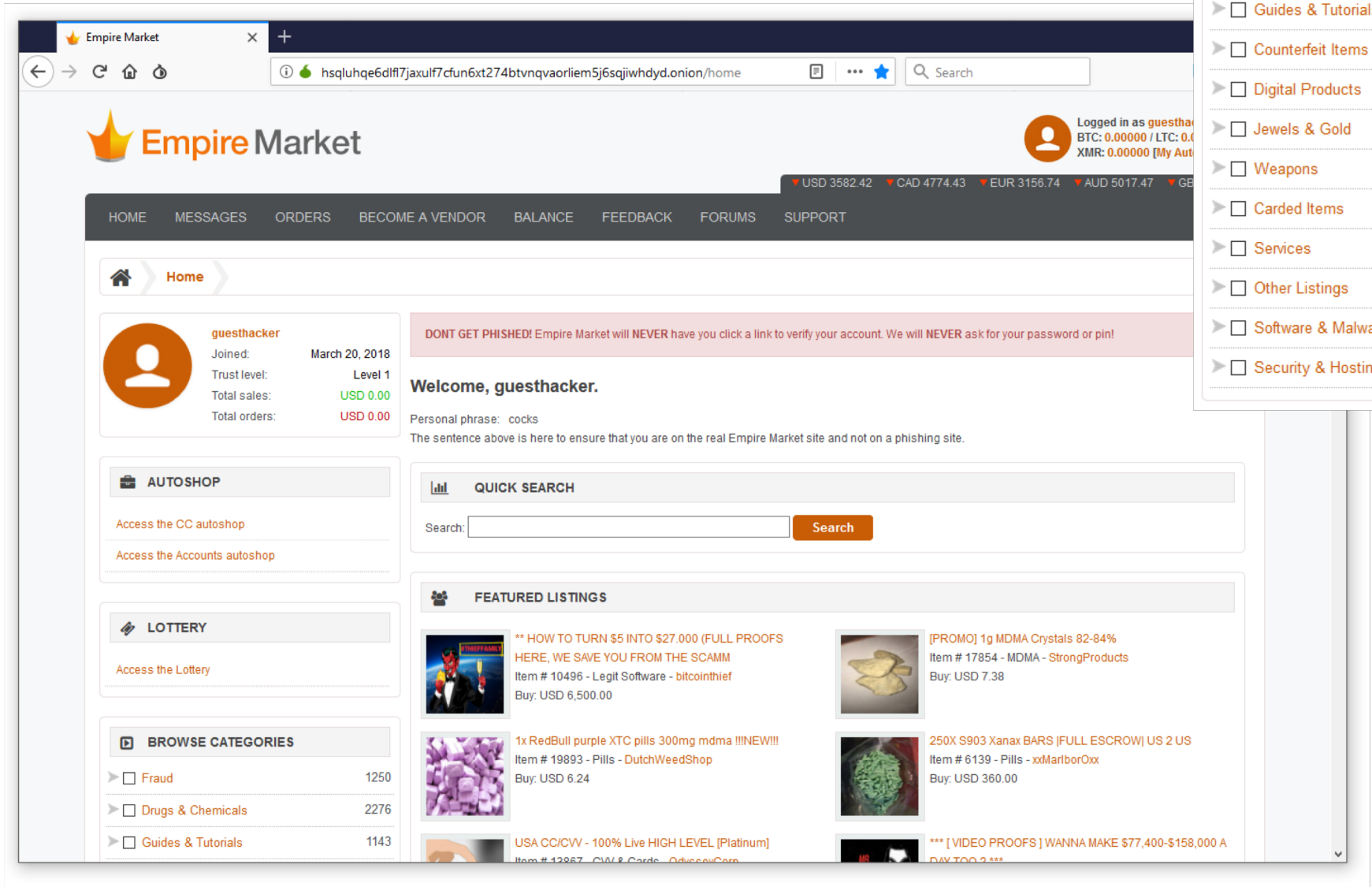


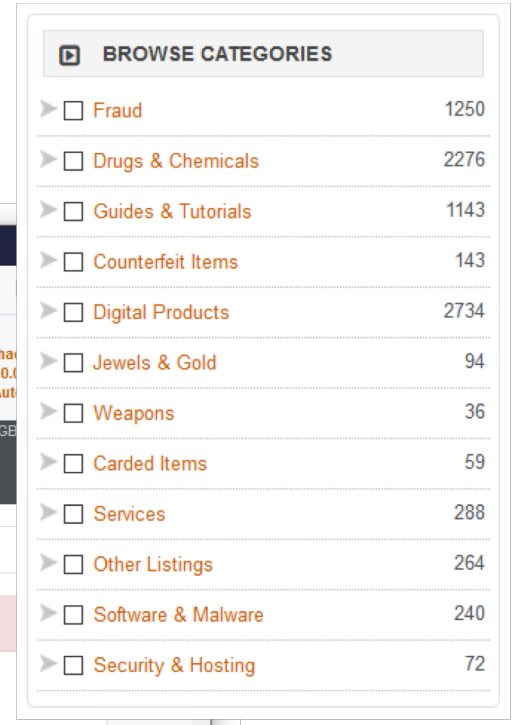
E-Commerce

- Black-market of the Internet
- Multiple categories
- Anonymous payments with crypto currieries
- Escrow services
- Legal/Illegal goods and services

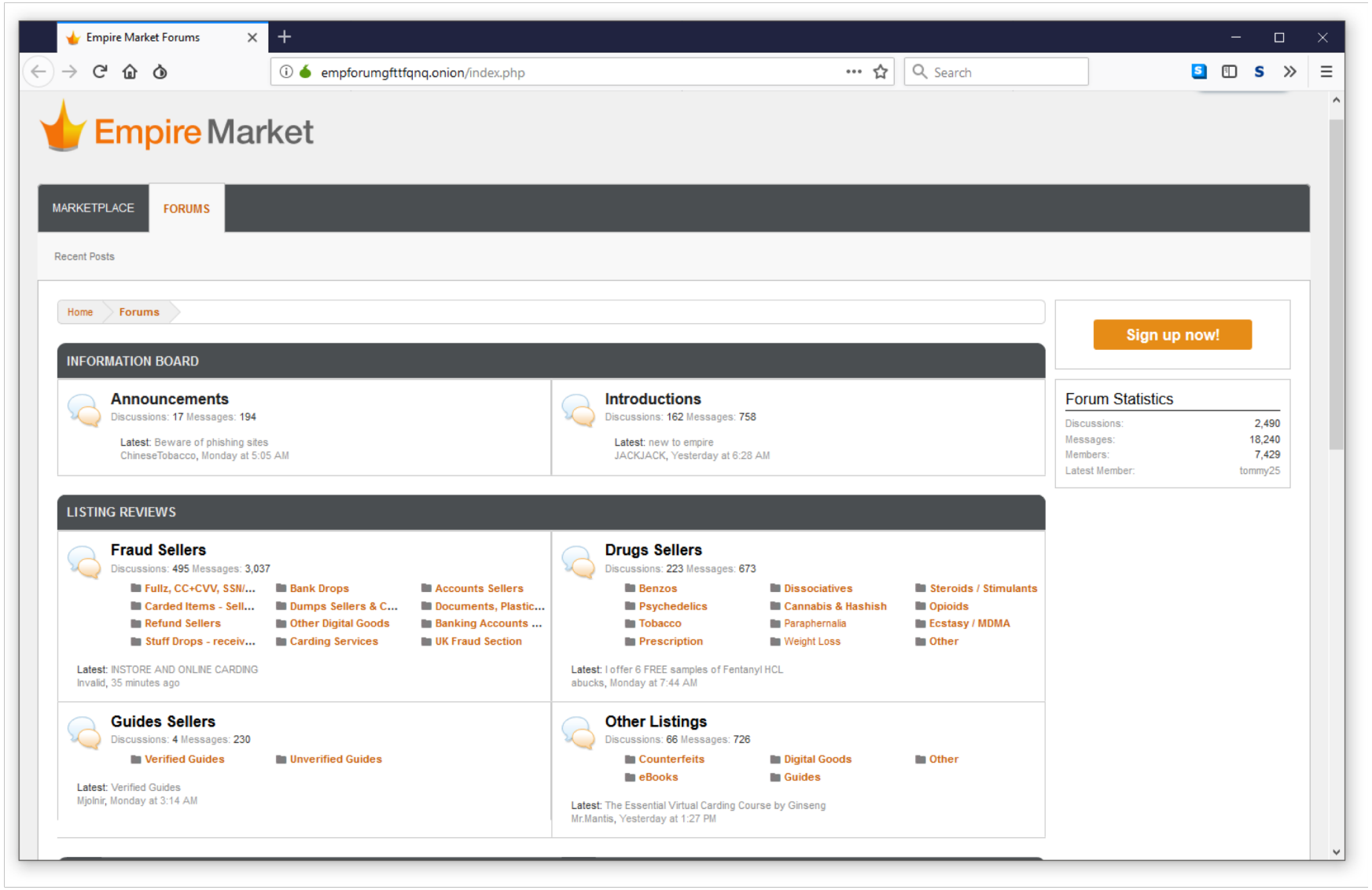


E-Commerce


Empire Market
hsqluhqe6dlfl7jaxulf7cfun6xt274btvnqvaorliem5j6sqjiwhdyd.onion/home
Search
Empire Market
Logged in as guesthacker
BTC: 0.00000 / LTC: 0.0
XMR: 0.00000 [My Auto
USD 3582.42
CAD 4774.43
EUR 3156.74
AUD 5017.47
HOME
MESSAGES
ORDERS
BECOME A VENDOR
BALANCE
FEEDBACK
FORUMS
SUPPORT
Home
guesthacker
Joined: March 20, 2018
Trust level: Level 1
Total sales: USD 0.00
Total orders: USD 0.00
DONT GET PHISHED! Empire Market will NEVER have you click a link to verify your account. We will NEVER ask for your password or pin!
Welcome, guesthacker.
Personal phrase: cocks
The sentence above is here to ensure that you are on the real Empire Market site and not on a phishing site.
AUTOSHOP
Access the CC autoshop
Access the Accounts autoshop
LOTTERY
Access the Lottery
BROWSE CATEGORIES
Fraud 1250
Drugs & Chemicals 2276
Guides & Tutorials 1143
QUICK SEARCH
Search:
Search
FEATURED LISTINGS
** HOW TO TURN $5 INTO $27.000 (FULL PROOFS HERE, WE SAVE YOU FROM THE SCAMM
Item # 10496 - Legit Software - bitcointhief
Buy: USD 6,500.00
[PROMO] 1g MDMA Crystals 82-84%
Item # 17854 - MDMA - StrongProducts
Buy: USD 7.38
1x RedBull purple XTC pills 300mg mdma !!!NEW!!!
Item # 19893 - Pills - DutchWeedShop
Buy: USD 6.24
250X S903 Xanax BARS |FULL ESCROW| US 2 US
Item # 6139 - Pills - xxMarlborOxx
Buy: USD 360.00
USA CC/CVV - 100% Live HIGH LEVEL [Platinum]
*** [VIDEO PROOFS] WANNA MAKE $77,400-$158,000 A

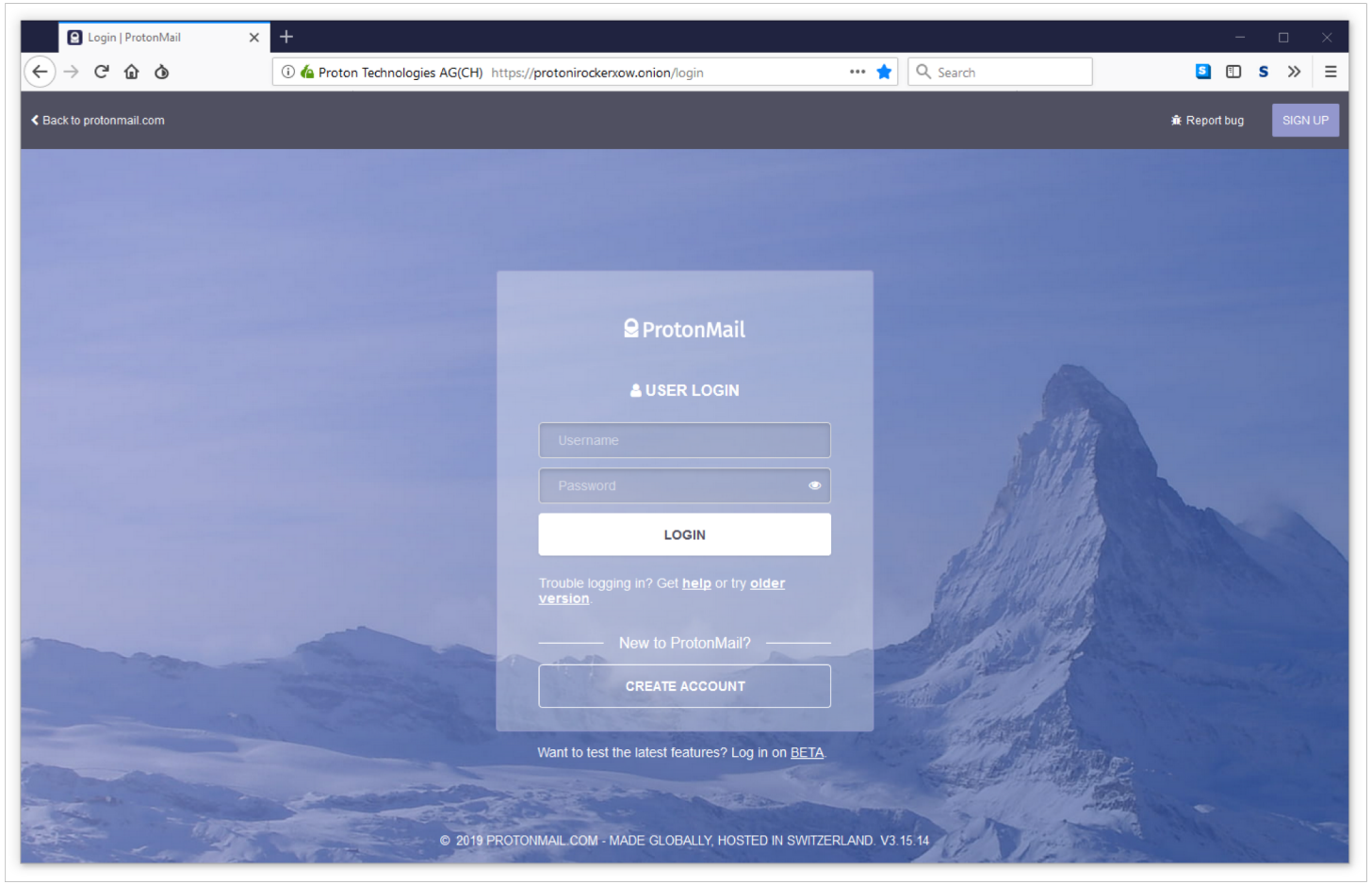

BROWSE CATEGORIES
Fraud 1250
Drugs & Chemicals 2276
Guides & Tutorials 1143
Counterfeit Items 143
Digital Products 2734
Jewels & Gold 94
Weapons 36
Carded Items 59
Services 288
Other Listings 264
Software & Malware 240
Security & Hosting 72

E-Commerce


Empire Market Forums
empforumgfttfqnq.onion/index.php
Search
Empire Market
MARKETPLACE
FORUMS
Recent Posts
Home
Forums
Sign up now!
INFORMATION BOARD
Announcements
Discussions: 17 Messages: 194
Latest: Beware of phishing sites
ChineseTobacco, Monday at 5:05 AM
Introductions
Discussions: 162 Messages: 758
Latest: new to empire
JACKJACK, Yesterday at 6:28 AM
Forum Statistics
Discussions: 2,490
Messages: 18,240
Members: 7,429
Latest Member: tommy25
LISTING REVIEWS
Fraud Sellers
Discussions: 495 Messages: 3,037
Fullz, CC+CVV, SSN/...
Bank Drops
Accounts Sellers
Carded Items - Sell...
Dumps Sellers & C...
Documents, Plastic...
Refund Sellers
Other Digital Goods
Banking Accounts ...
Stuff Drops - receiv...
Carding Services
UK Fraud Section
Latest: INSTORE AND ONLINE CARDING
Invalid, 35 minutes ago
Drugs Sellers
Discussions: 223 Messages: 673
Benzos
Dissociatives
Steroids / Stimulants
Psychedelics
Cannabis & Hashish
Opioids
Tobacco
Paraphernalia
Ecstasy / MDMA
Prescription
Weight Loss
Other
Latest: I offer 6 FREE samples of Fentanyl HCL
abucks, Monday at 7:44 AM
Guides Sellers
Discussions: 4 Messages: 230
Verified Guides
Unverified Guides
Latest: Verified Guides
Mjolnir, Monday at 3:14 AM
Other Listings
Discussions: 66 Messages: 726
Counterfeits
Digital Goods
Other
eBooks
Guides
Latest: The Essential Virtual Carding Course by Ginseng
Mr.Mantis, Yesterday at 1:27 PM

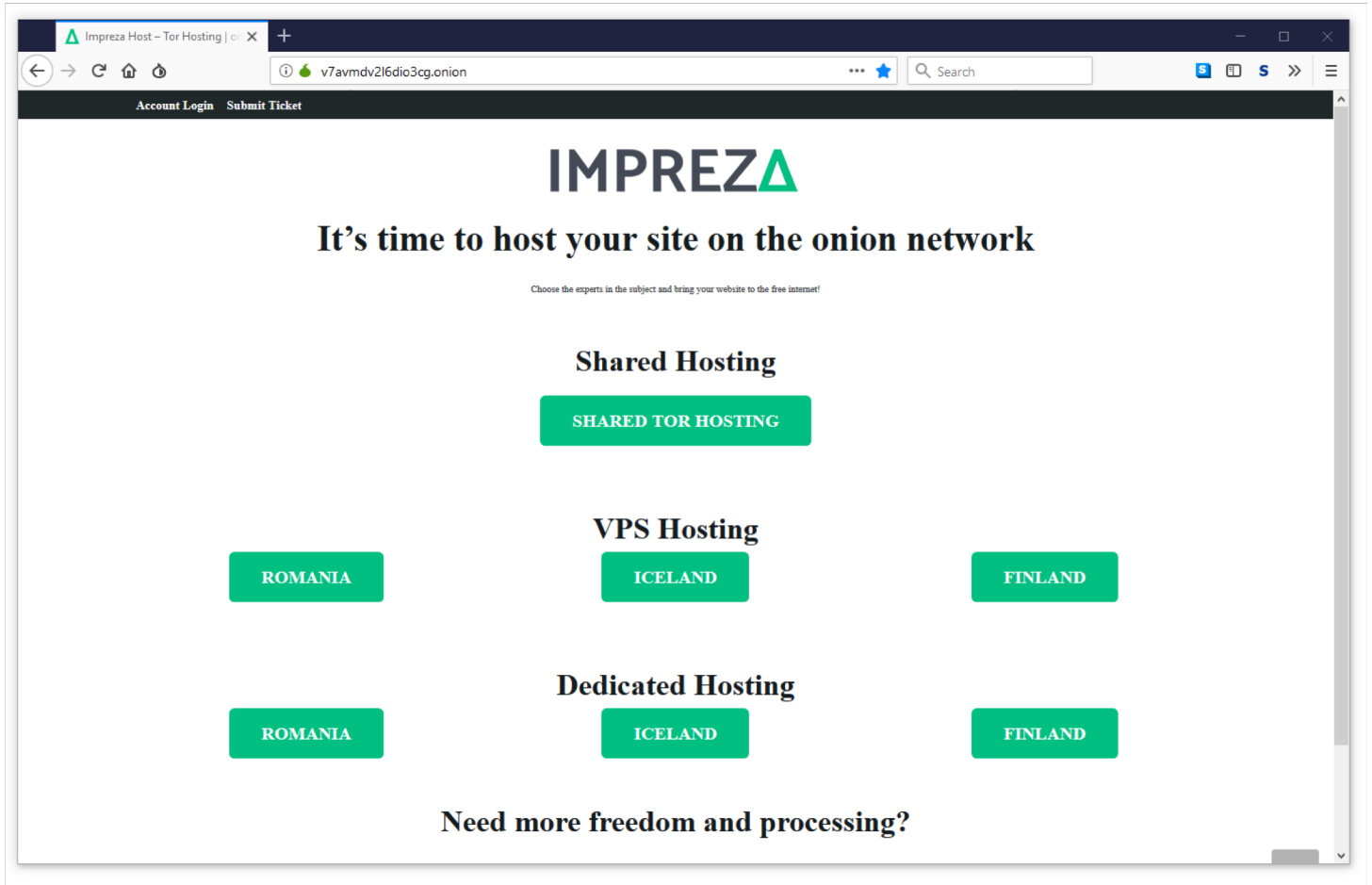
Email Services

- Tor adds an additional layer of security
- Combats Censorship and Surveillance
- Options
  - Tor only service
  - Clearnet services with hidden service option

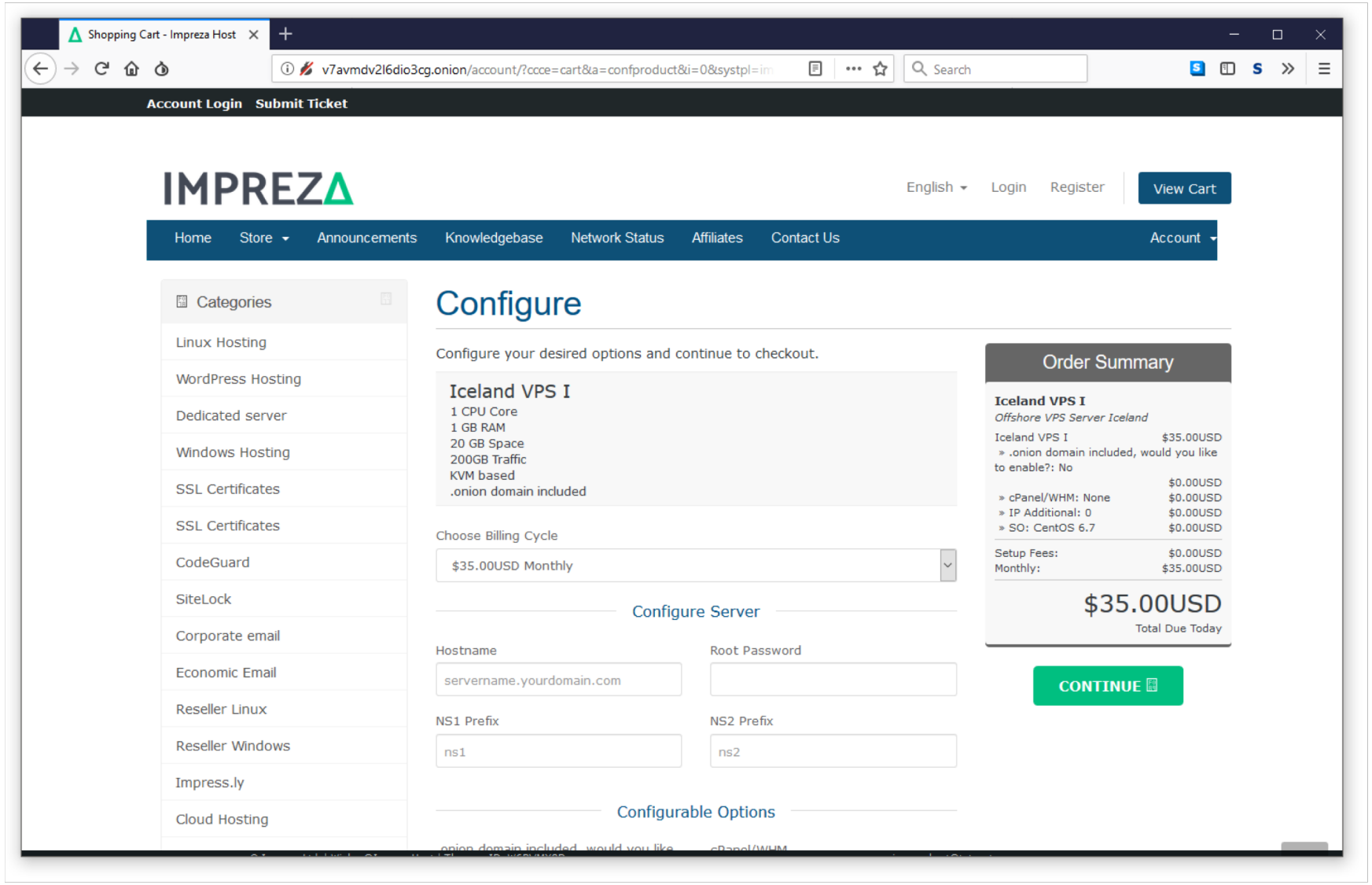


Hosting Services

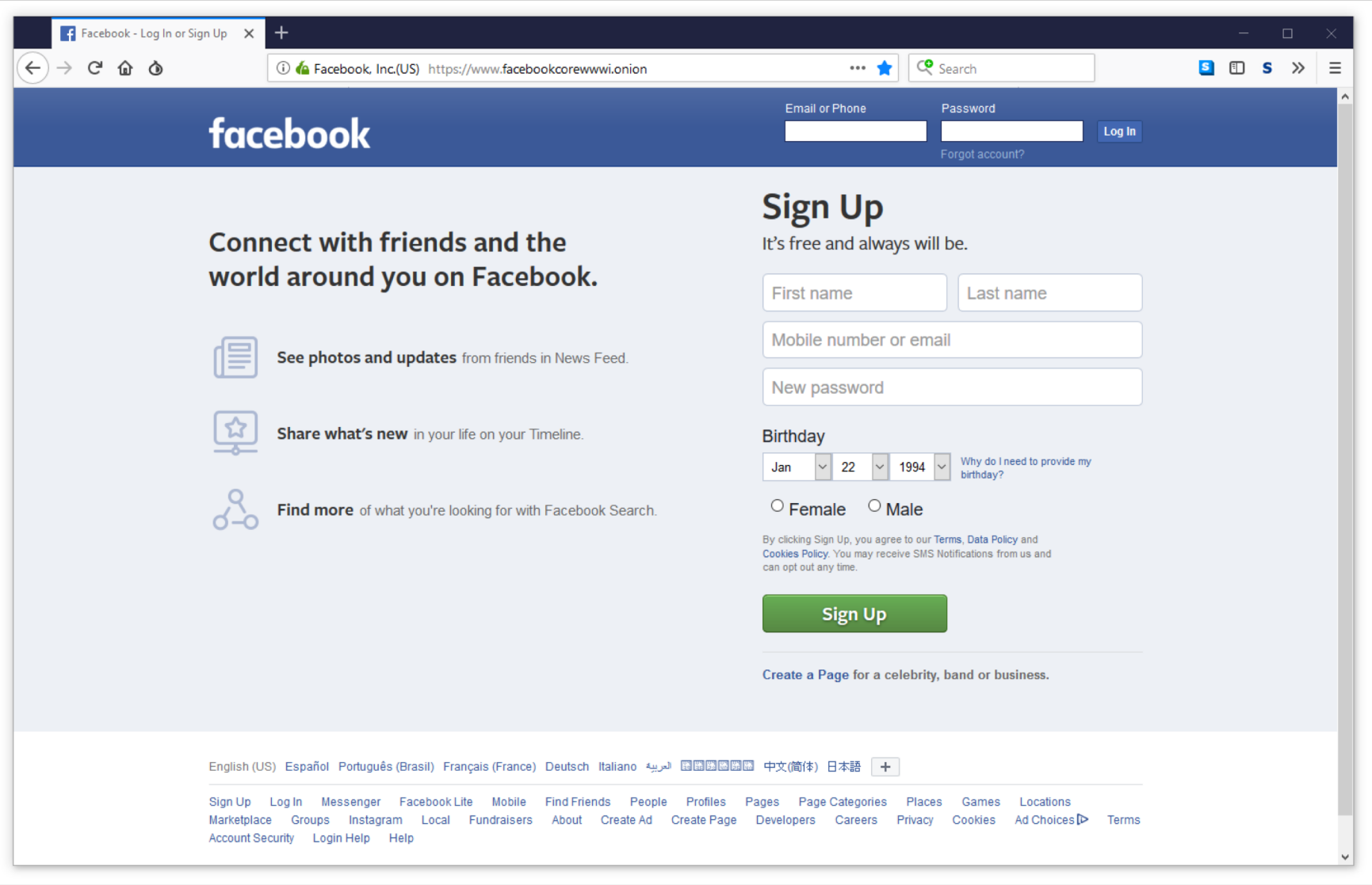
- Risk Analysis / Trust
- High-Privacy hosting
  - Bulletproof / Offshore hosting
- Option
  - Self host on a VPS



Hosting Services

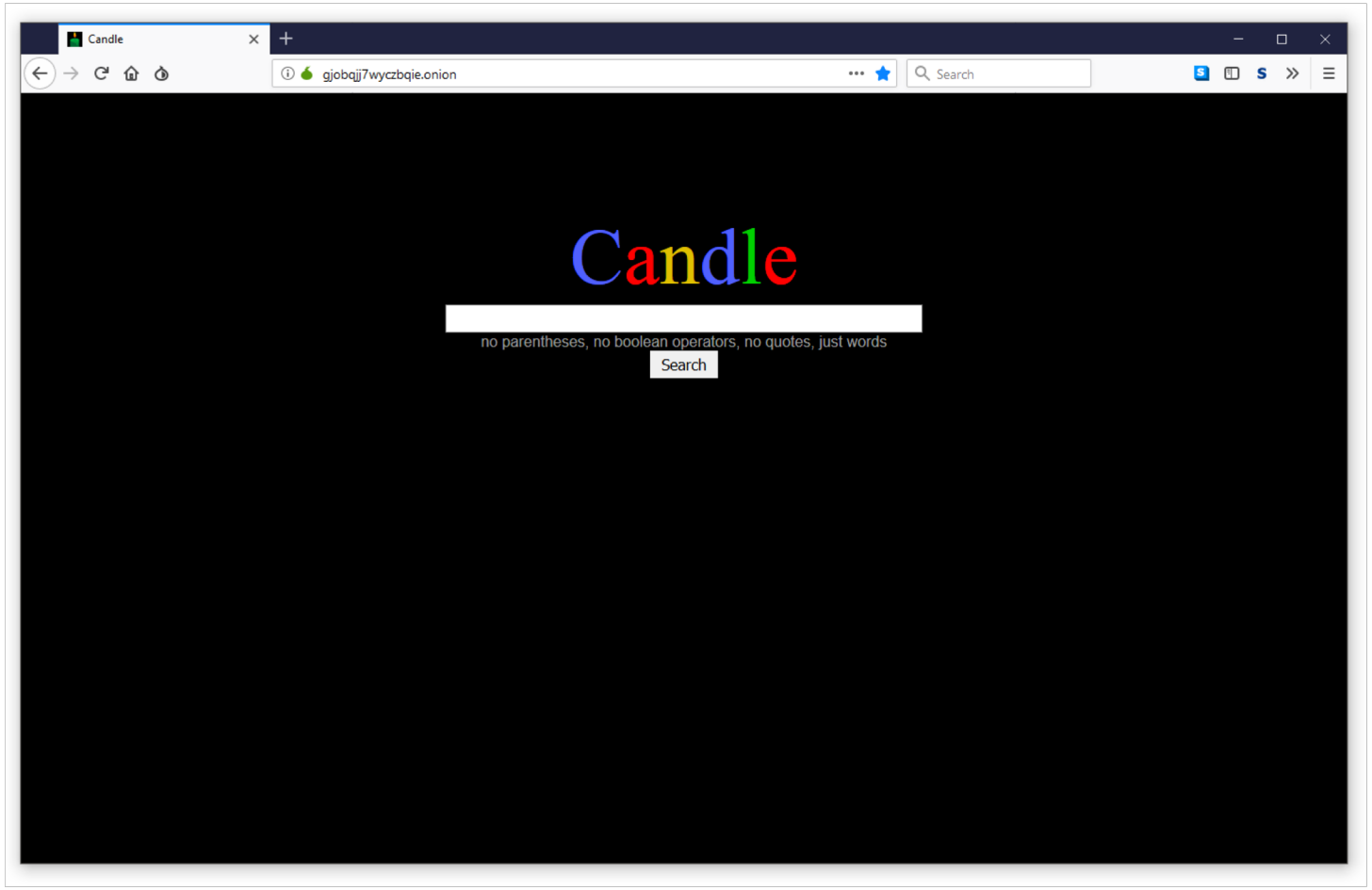


Facebook

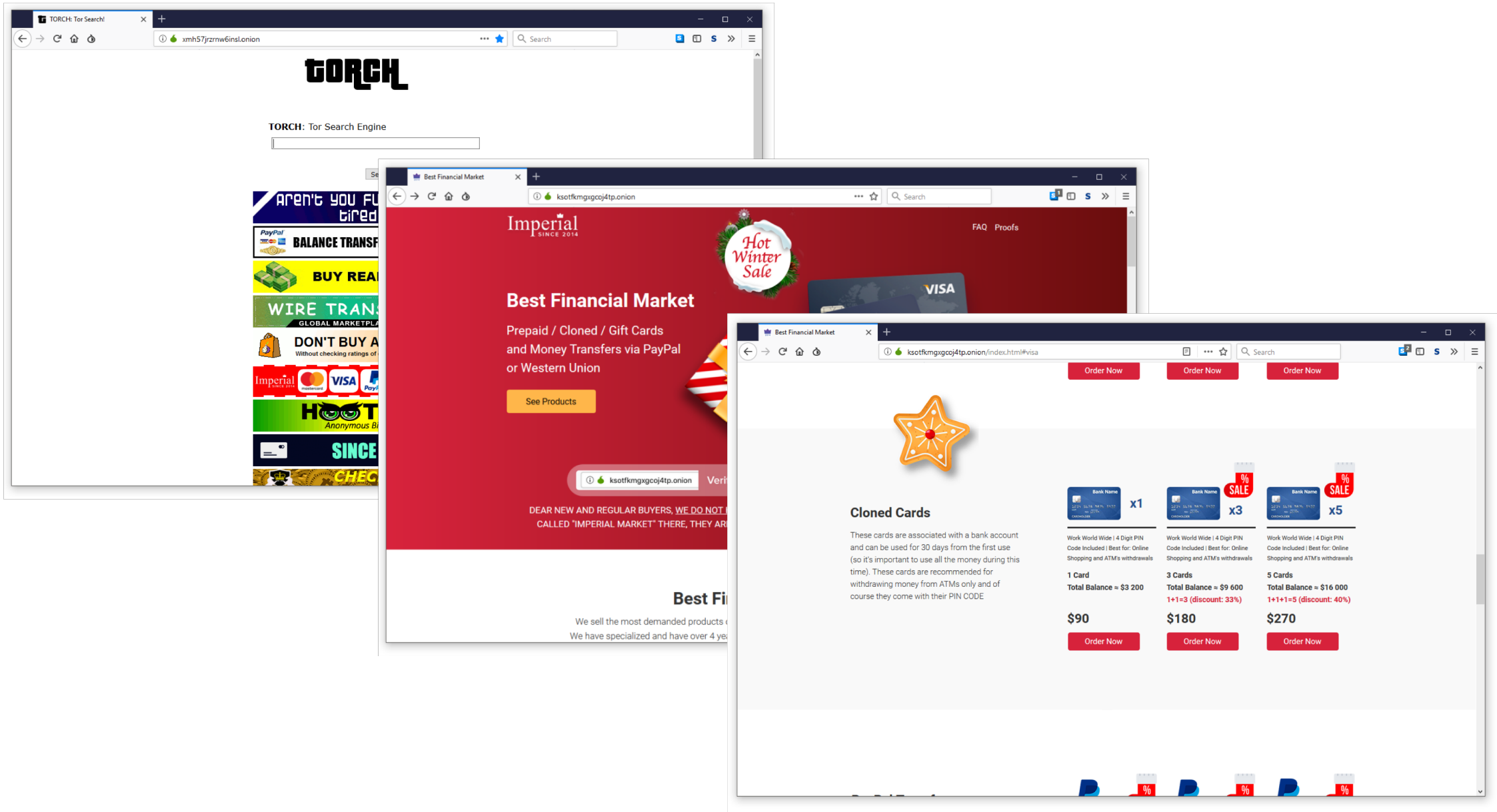

Facebook - Log In or Sign Up
Facebook, Inc.(US) https://www.facebookcorewwwi.onion
Search
facebook
Email or Phone
Password
Log In
Forgot account?
Connect with friends and the world around you on Facebook.
See photos and updates from friends in News Feed.
Share what's new in your life on your Timeline.
Find more of what you're looking for with Facebook Search.
Sign Up
It's free and always will be.
First name
Last name
Mobile number or email
New password
Birthday
Jan
22
1994
Why do I need to provide my birthday?
Female
Male
By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.
Sign Up
Create a Page for a celebrity, band or business.
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية 中文(简体) 日本語
Sign Up Log In Messenger Facebook Lite Mobile Find Friends People Profiles Pages Page Categories Places Games Locations
Marketplace Groups Instagram Local Fundraisers About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices Terms
Account Security Login Help Help

Search Engines

- Indexed .onion sites
- Easier to search for Hidden Services



Search Engines



Agenda

- What is the Darknet
- How to access the Darknet
- What can you find
- What can you buy
- **Why hackers use the Darknet**

Why hackers use the Darknet?

Benefits of the Darknet to an attacker:

- Privacy
- Obfuscation
- Opportunity

radware

Thank You