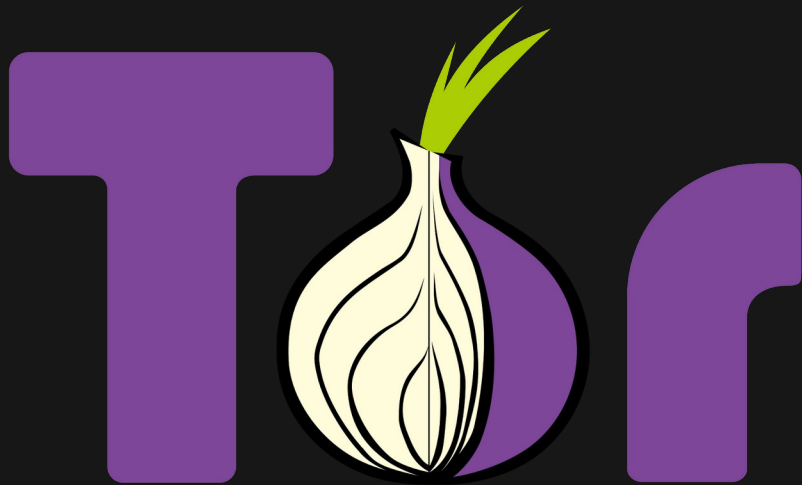
Intro to Tor

Jaxon Haws



Congrats! You’re now **probably** on a government watchlist!

DISCLAIMER

DON’T DO ANYTHING TO GET YOURSELF ARRESTED

Yay! I always wanted to be on a government watchlist!

2ND DISCLAIMER

MORE IMPORTANTLY, DON'T DO ANYTHING TO GET *ME* ARRESTED

Table of Contents

What isn’t Tor?

- The Dark Web
- The Deep Web
- Illegal (at least in the U.S.)
- A VPN
- Torrenting
- Completely foolproof

What is Tor?

- Tor – The Onion Router
- Free and open-source software for enabling anonymous communication
- Can be used in the form of a proxy for individual applications/whole system or as a browser
- Tor directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than six thousand relays

Tor History

- 1995 – Concept of onion routing was created
- 2002 – Tor network began being deployed
- 2006 – Tor project founded by computer scientists Roger Dingledine, Nick Mathewson and five others
- 2008 – Tor browser was released
- 2013 – Edward Snowden used Tor

Tor based operating systems

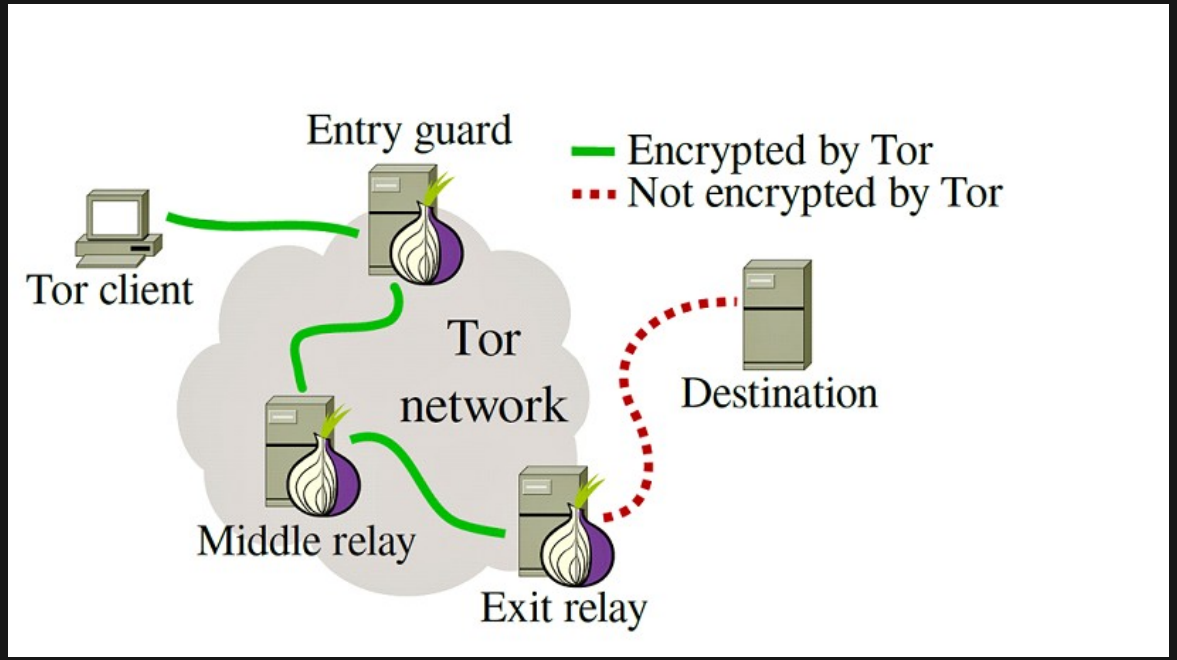
- Tails
- Whonix
- Qubes OS

How does Tor work?

Tor Nodes: Guards, Bridges, Relays, & Exit Nodes

- Guards
  - Publicly Registered Entry Nodes
  - Forward request/data to relay from users
- Bridges
  - Privately Registered Entry Nodes
- Relays
  - Middleman: receive requests from other nodes and forwards them to another node
- Exit Nodes
  - Sends content to final location/server/website
  - Retrieves content from final location/server/website and sends to relay

The Onion Router



Onion Services (*.onion)

- Basically URLs, generated based on a public key when an onion service is configured
- 16 characters long for V2 (base32 80 bit hash)
- 56 characters long for V3 (256-bit ed25519 public key, version number, and a checksum)
- Strings containing any letter and/or digits 2-7
- Require onion routing to access

What can you browse with Tor?

Surface web

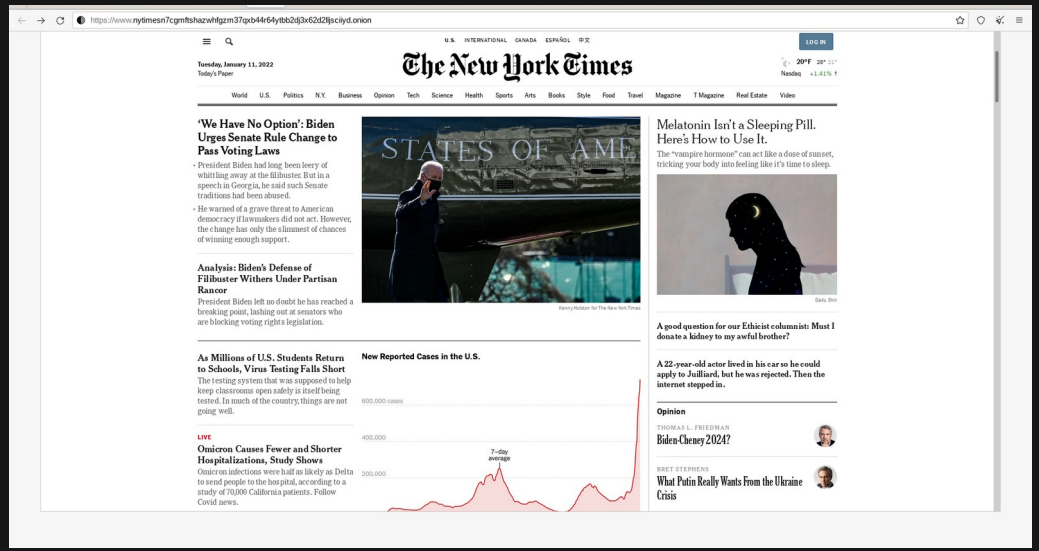
- Any public websites indexed by a search engine
  - duckduckgo.com
  - eff.org
  - torproject.org
  - cpsecurity.club
  - cplug.org

Deep web

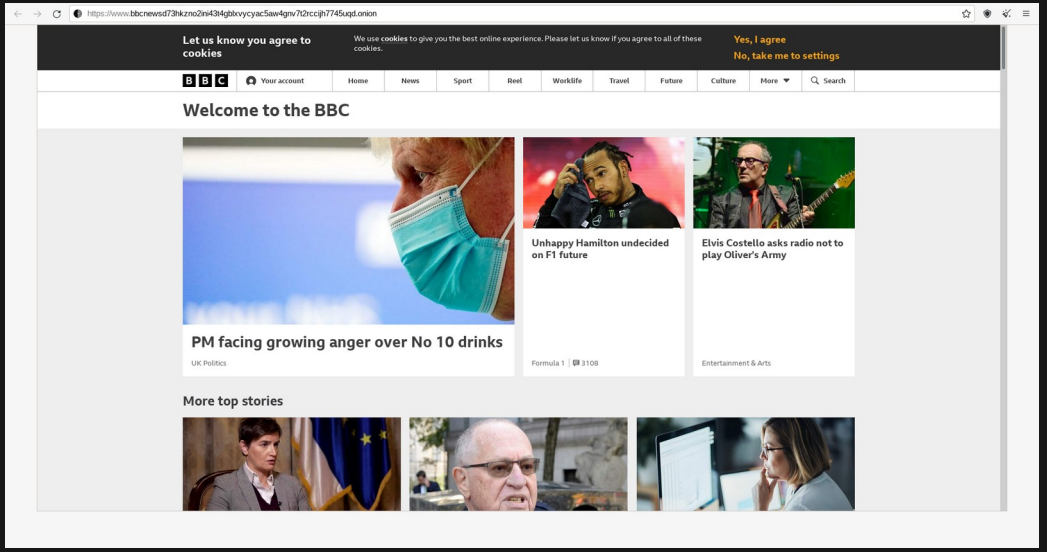
- Anything that is not indexed by publicly accessible search engines
- Onion sites
  - See examples ->

Journalism

- https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion

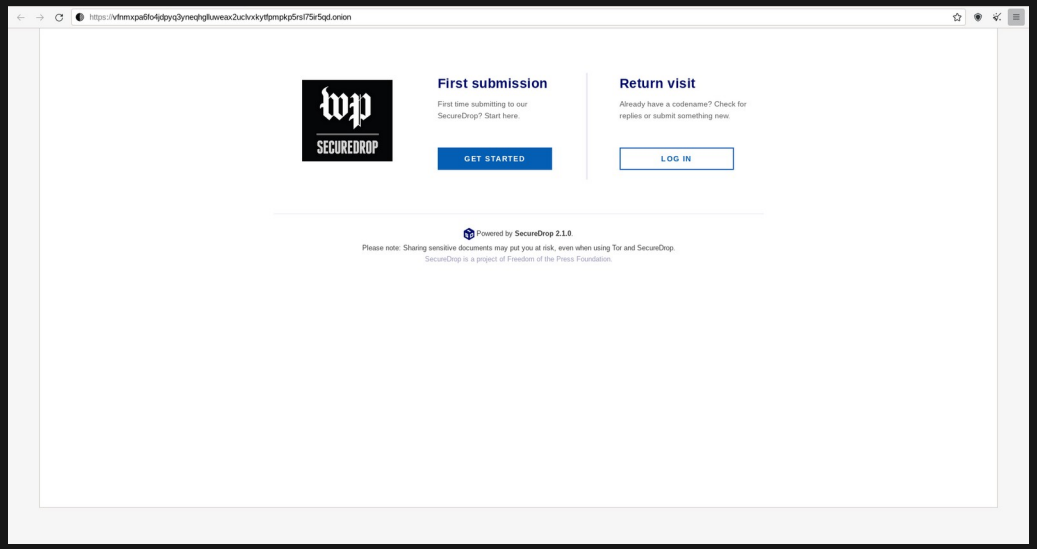


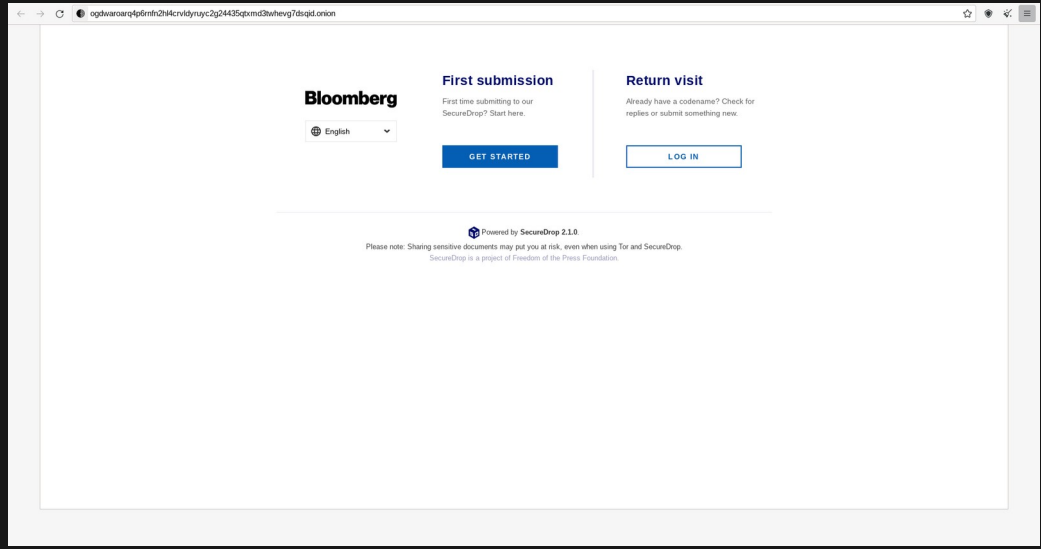
- https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion



SecureDrops

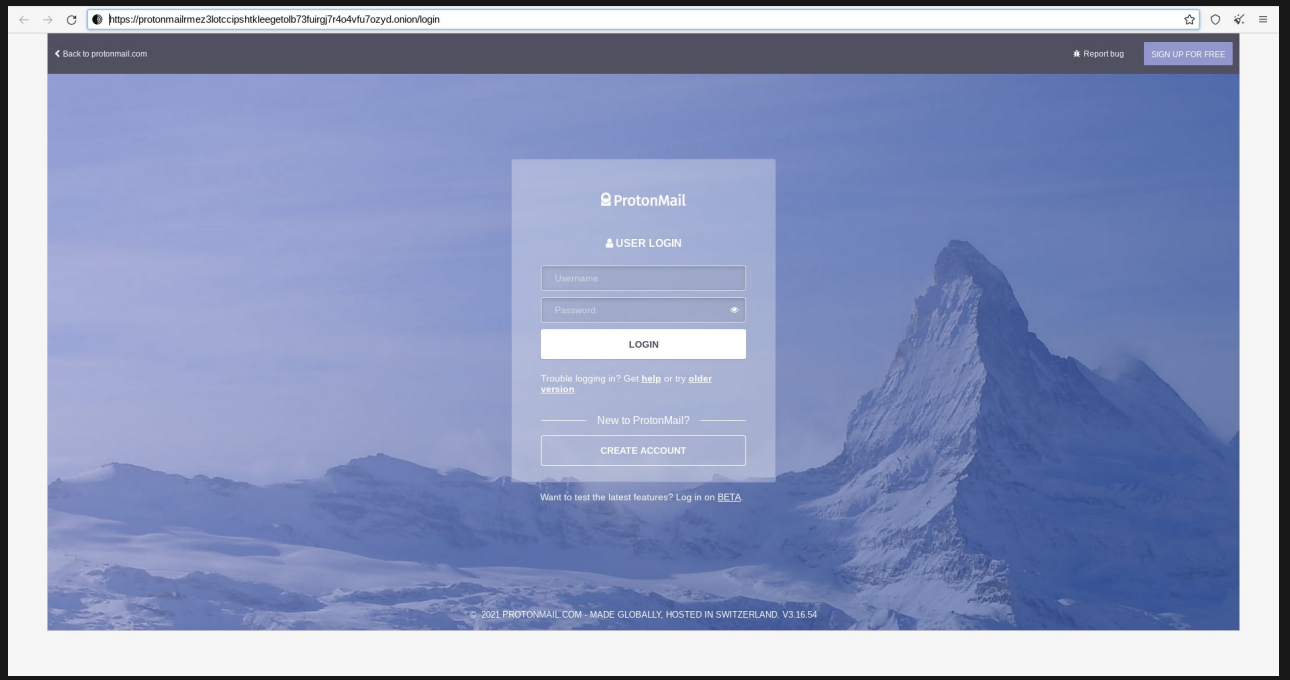
- https://vfnmxpa6fo4jdpyq3yneqhglluweax2uclvxkytfpmpkp5rsl75ir5qd.onion
- http://ogdwaroarq4p6rnfn2hl4crvldyruyc2g24435qtxmd3twhevg7dsqid.onion





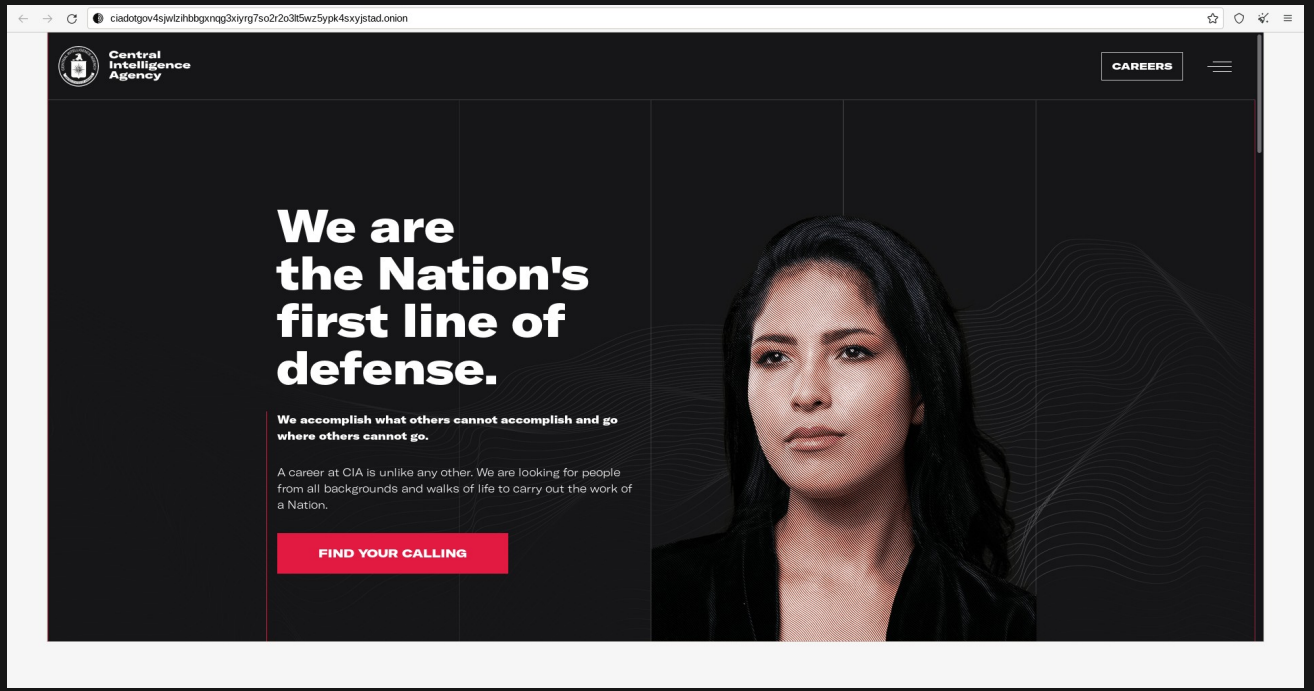
Email

- https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion



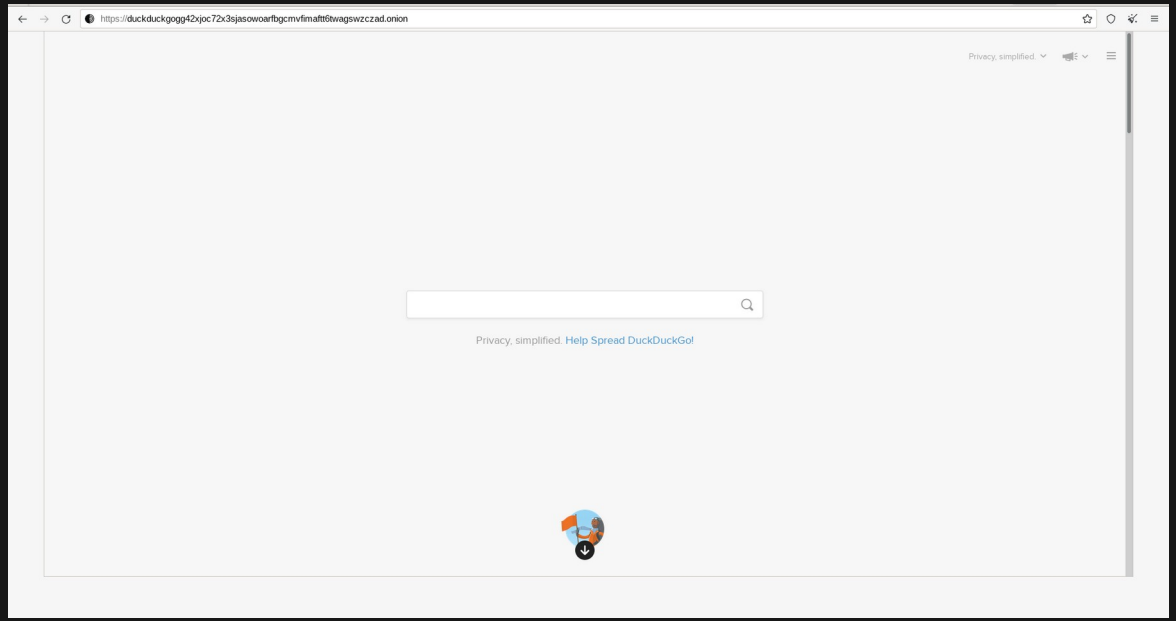
Law Enforcement

- http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion

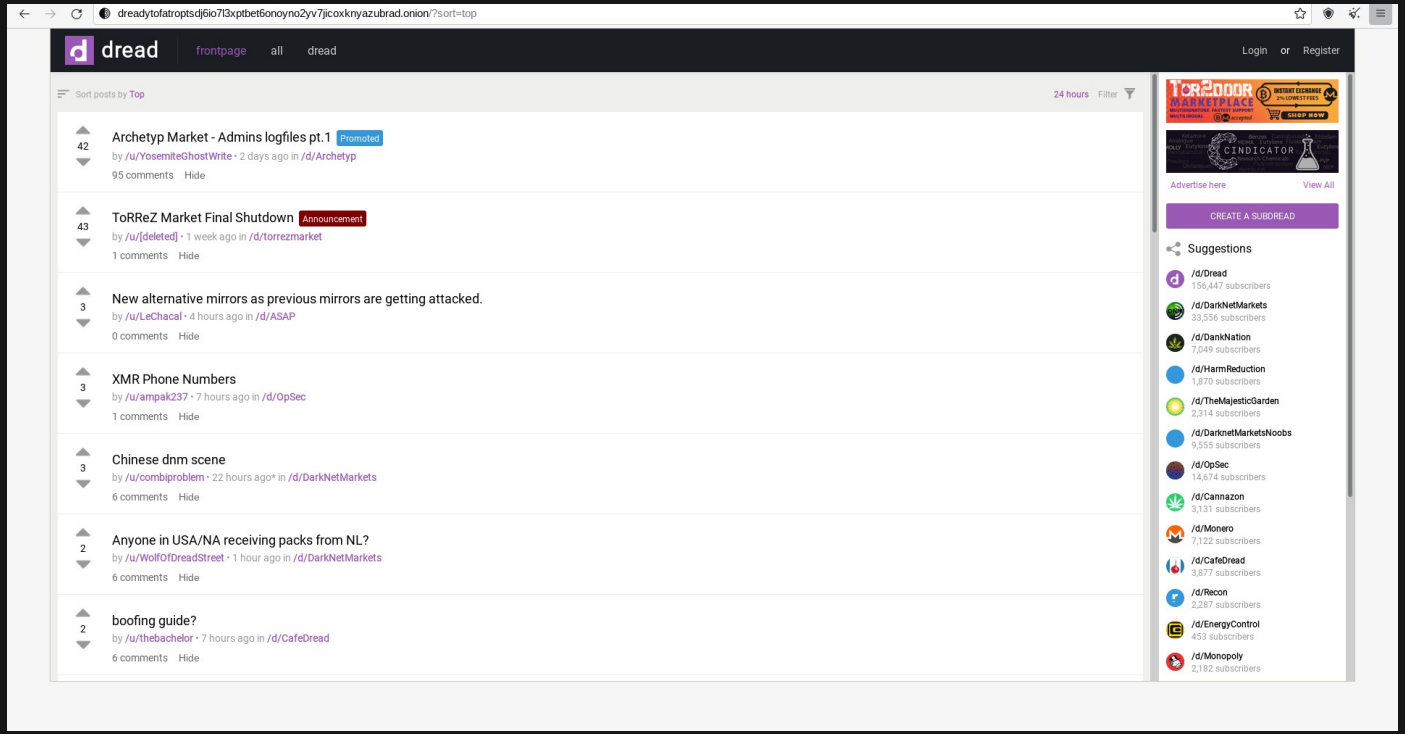


Search Engines

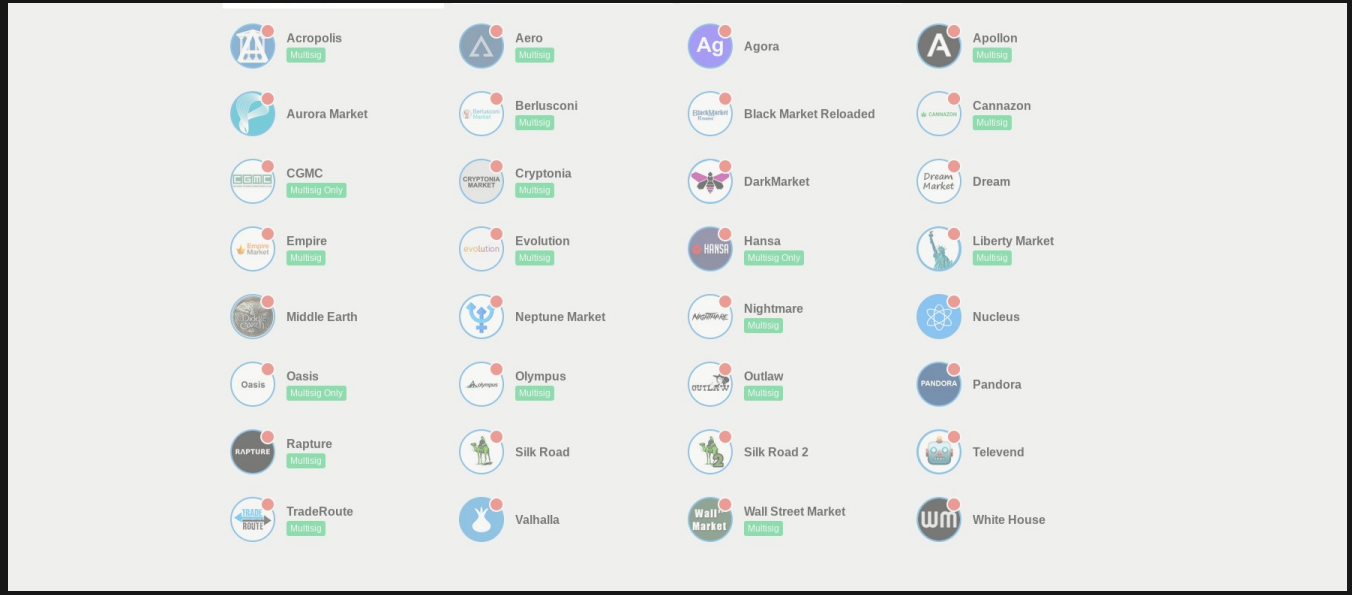
- https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion



Forums

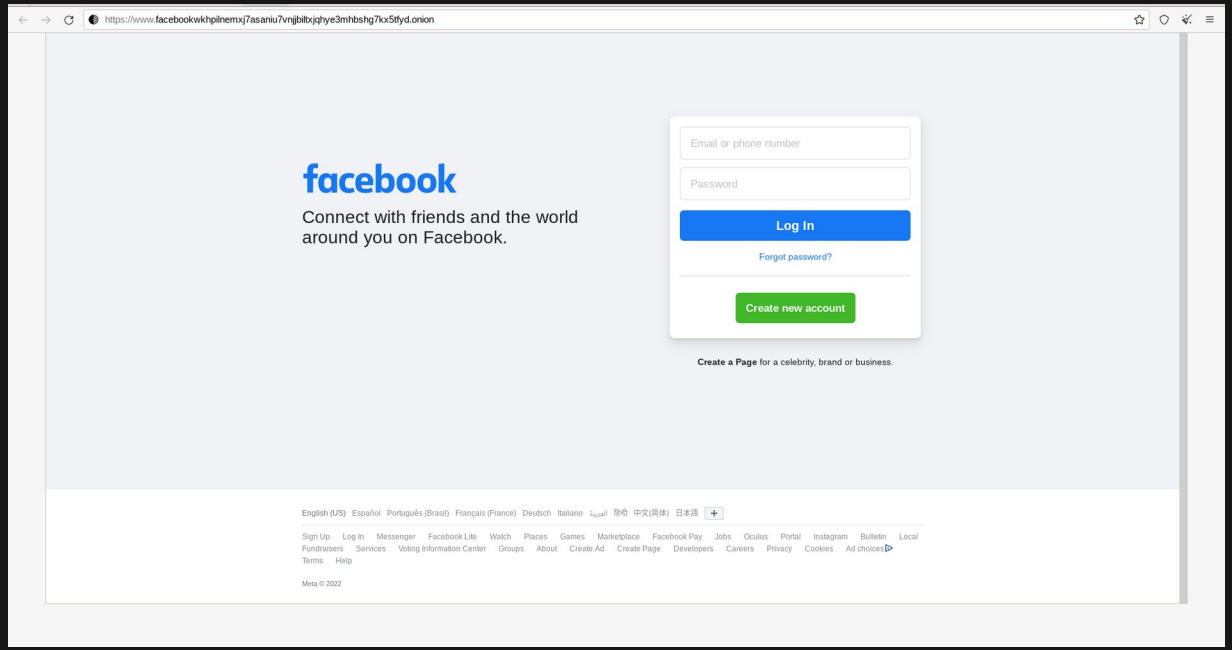

dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/?sort=top
dread
frontpage
all
dread
Login or Register
Sort posts by Top
24 hours Filter
42
Archetyp Market - Admins logfiles pt.1 Promoted
by /u/YosemiteGhostWrite • 2 days ago in /d/Archetyp
95 comments Hide
43
ToRReZ Market Final Shutdown Announcement
by /u/[deleted] • 1 week ago in /d/torrezmarket
1 comments Hide
3
New alternative mirrors as previous mirrors are getting attacked.
by /u/LeChacal • 4 hours ago in /d/ASAP
0 comments Hide
3
XMR Phone Numbers
by /u/ampak237 • 7 hours ago in /d/OpSec
1 comments Hide
3
Chinese dnm scene
by /u/combiproblem • 22 hours ago* in /d/DarkNetMarkets
6 comments Hide
2
Anyone in USA/NA receiving packs from NL?
by /u/WolfOfDreadStreet • 1 hour ago in /d/DarkNetMarkets
6 comments Hide
2
boofing guide?
by /u/thebachelor • 7 hours ago in /d/CafeDread
6 comments Hide
Advertise here
View All
CREATE A SUBDREAD
Suggestions
/d/Dread
156,447 subscribers
/d/DarkNetMarkets
33,556 subscribers
/d/DankNation
7,049 subscribers
/d/HarmReduction
1,870 subscribers
/d/TheMajesticGarden
2,314 subscribers
/d/DarknetMarketsNoobs
9,555 subscribers
/d/OpSec
14,674 subscribers
/d/Cannazon
3,131 subscribers
/d/Monero
7,122 subscribers
/d/CafeDread
3,877 subscribers
/d/Recon
2,287 subscribers
/d/EnergyControl
453 subscribers
/d/Monopoly
2,182 subscribers

Marketplaces?



Facebook?

- https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion



How secure is Tor?

Pretty secure

- Problems really only exist at entry/exit nodes

Browser Fingerprinting

- A digital fingerprint is created when a company makes a unique profile of you based on your computer hardware, software, add-ons, and even preferences.
- Tor browser sessions are designed to all look identical
- See your browser’s fingerprint here:
  - Coveryourtracks.eff.org

Browser Fingerprinting:

Personal Firefox vs Tor Browser

Our tests indicate that you have **strong protection against Web tracking**.

IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 220,702 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.75 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

Our tests indicate that you have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.

IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a non-unique fingerprint

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 606.32 browsers have the same fingerprint as yours.**

Currently, we estimate that your browser has a fingerprint that conveys **9.24 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

Sources

- https://www.torproject.org/
- https://wiki.archlinux.org/title/Tor
- https://hackernoon.com/how-does-tor-really-work-c3242844e11f
- https://www.reddit.com/r/onions/
- https://www.reddit.com/r/TOR/
- https://en.wikipedia.org/wiki/Tor_(network)
- https://en.wikipedia.org/wiki/.onion