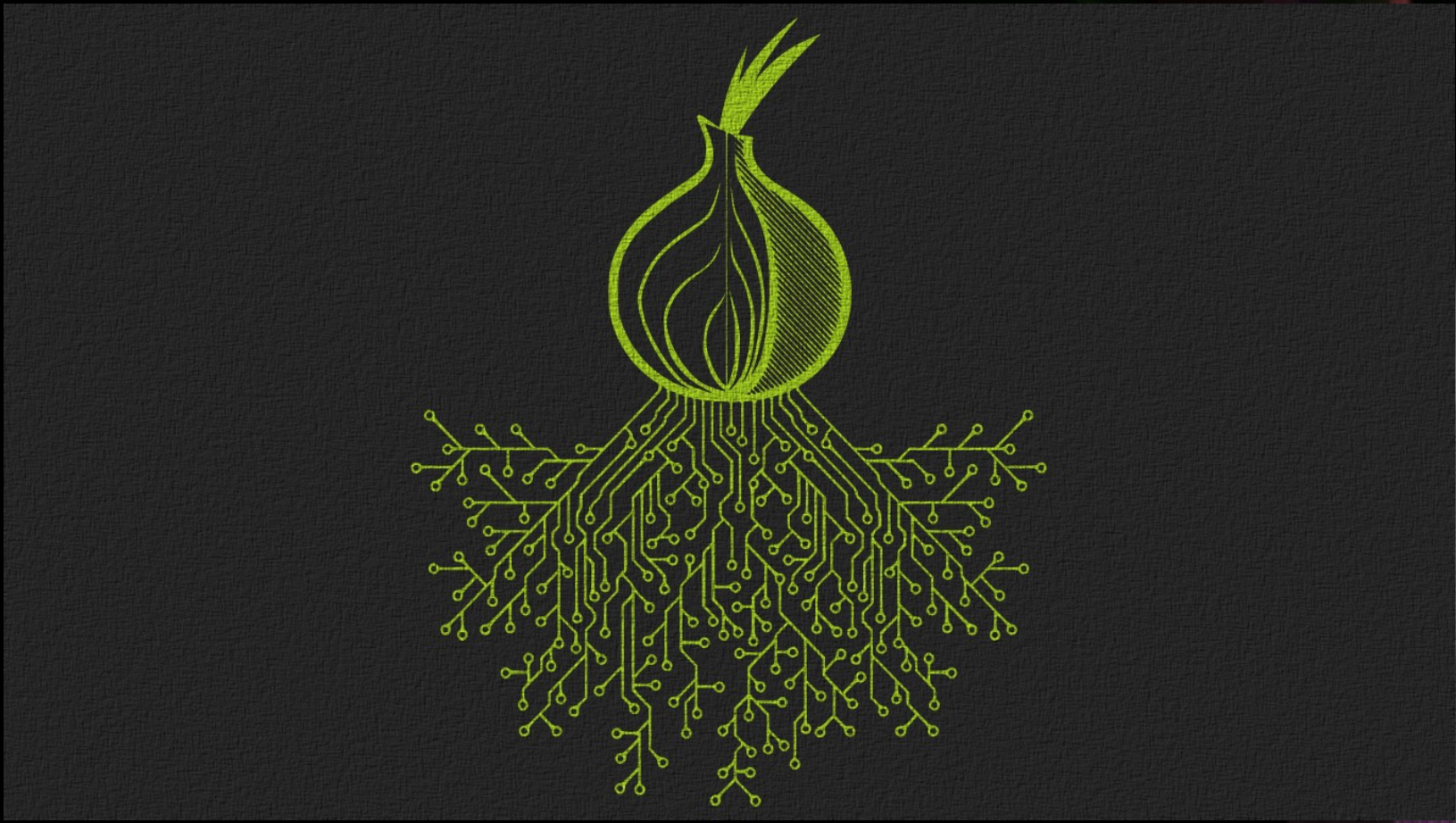
Tor: Anonymity, tools, and operational security



Micah Lee
@micahflee
927F419D7EC82C2F149C1BD1403C2657CD994F73

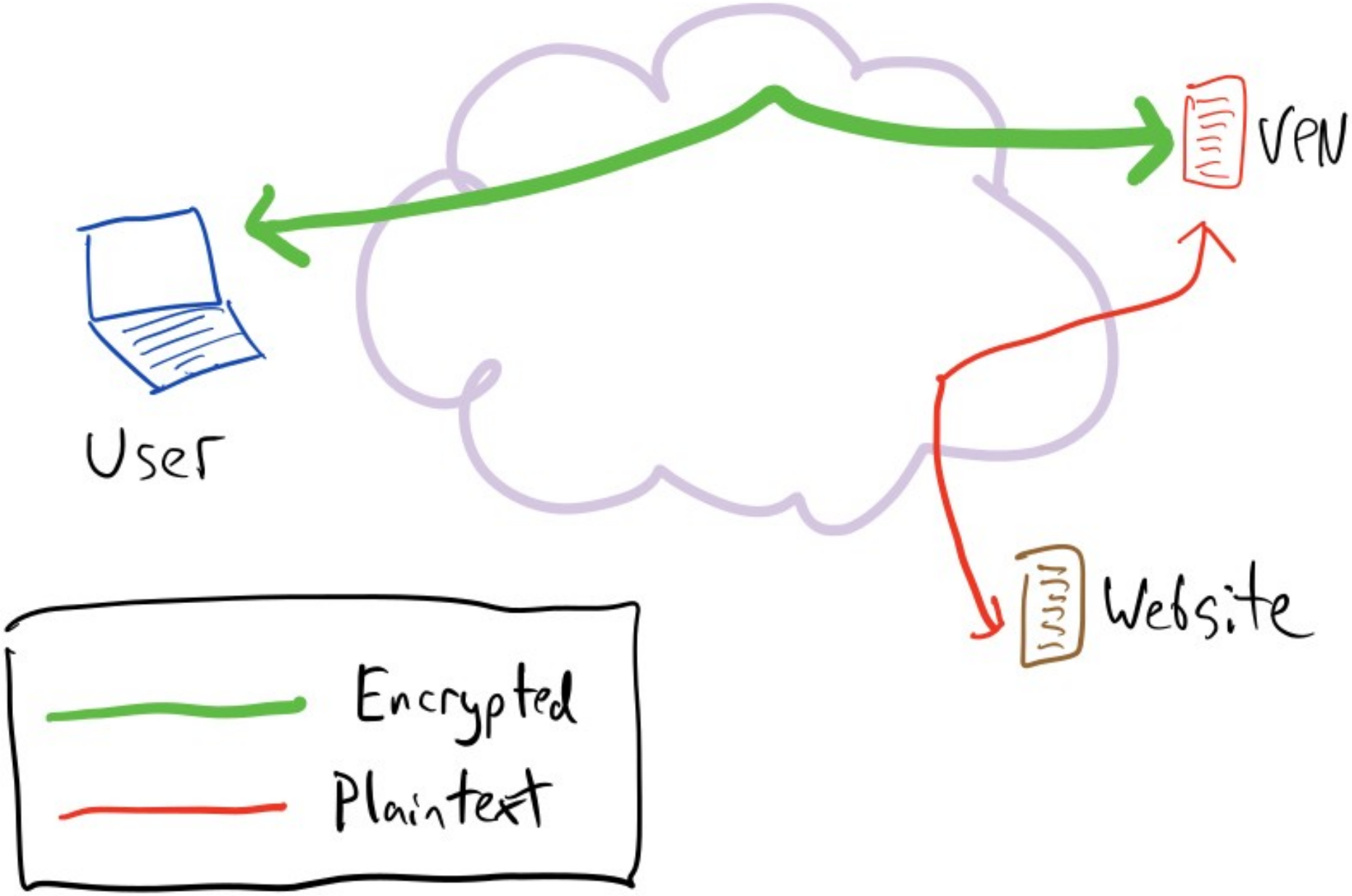
What is Tor?

- Tor is both a piece of open source software, and a network of servers run by volunteers (like me)
- **Tor allows anyone to make TCP connections over the internet while hiding their IP address**
- **Tor onion services** allow for anonymous network services (and bypass NAT)
- Tor is useful for **censorship circumvention**, **defense against surveillance**, and **real private browser/incognito mode**

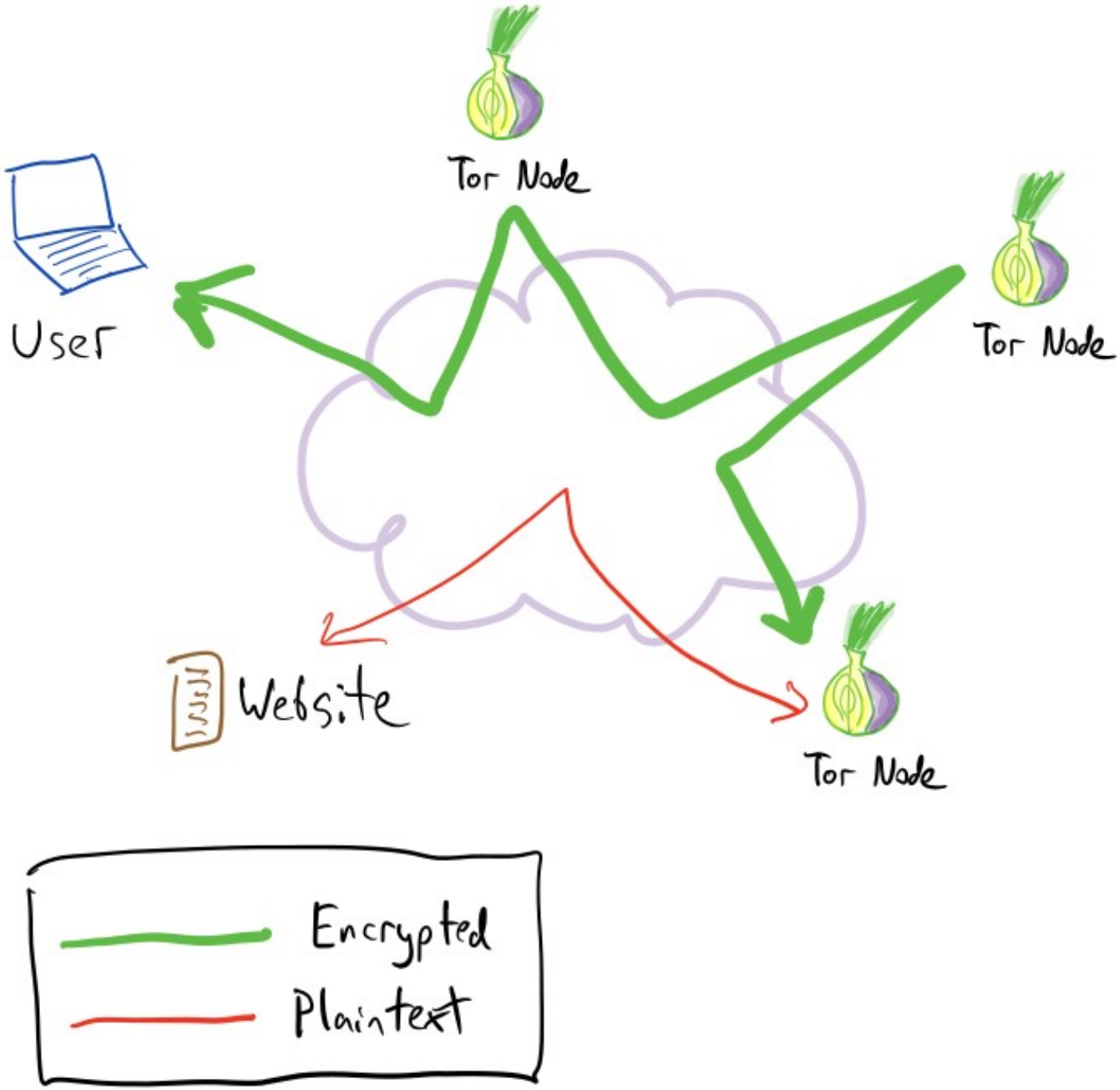
How does Tor work?

- When you use Tor, you are part of an **anonymity set** of ~2,000,000 monthly active users. The network has ~6,200 volunteer nodes.
- **Tor Browser** protects you from **browser fingerprinting**, and doesn’t leave a trace of your browsing history on disk
- **Tor circuits** contain 3 nodes:
  - The entry node knows who you are, but not what you’re doing
  - The middle node doesn’t know who you are or what you’re doing
  - The exit node doesn’t know who you are, but can see what you’re doing

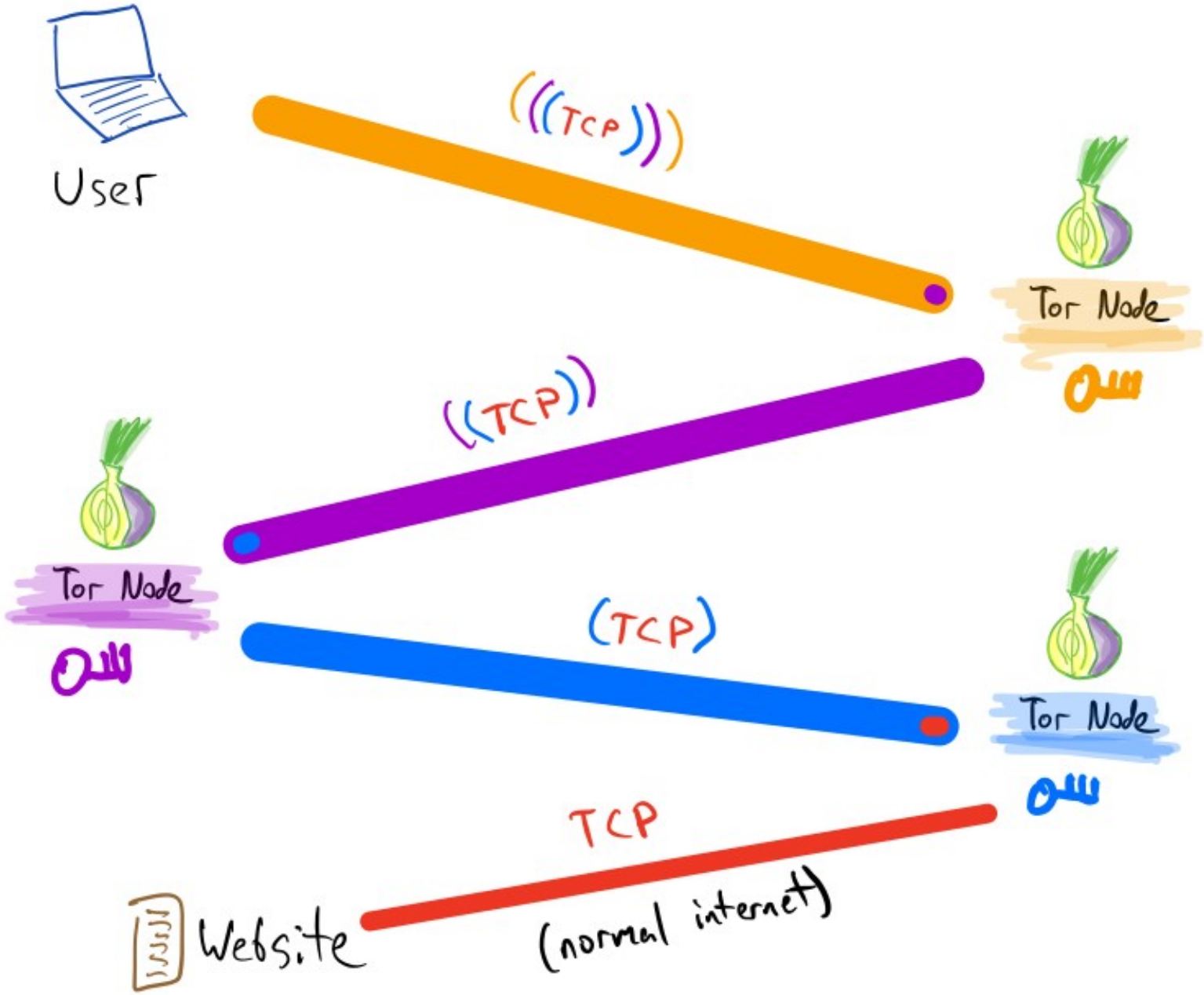
How VPNs Work



How Tor Works



Layers of Encryption



Tor Browser

- Based on **Firefox**
- Includes custom add-ons (Torbutton, TorLauncher), and privacy/security add-ons (HTTPS Everywhere, NoScript)
- Runs **tor** as a background process
  - SOCKS port: 9150
  - Control port: 9151
- It's simple to configure Firefox, Chrome, or other browsers to use Tor, but **don't do it** – Tor Browser protects from browser fingerprinting and doesn't leave forensic traces

GitHub - micahflee/torbrowser-launcher: Securely and easily download, verify, install, and launch Tor Browser in Linux - Tor Browser

File Edit View History Bookmarks Tools Help

GitHub - micahflee/torbro

GitHub, Inc. (US) https://github.com/micahflee/torbrowser-launcher

Why GitHub? Enterprise Explore Marketplace Pricing Search Sign in Sign up

micahflee / torbrowser-launcher

Watch 38 Star 294 Fork 71

Code Issues 54 Pull requests 6 Projects 0 Wiki Insights

Securely and easily download, verify, install, and launch Tor Browser in Linux

687 commits 3 branches 39 releases 38 contributors View license

Branch: develop New pull request Find file Clone or download

micahflee Add warning about errors to readme, and update screenshot Latest commit 326669f 9 days ago

.github	Add @intrigeri as code owner for AppArmor profiles	10 months ago
apparmor	AppArmor: give Web Content processes read access to the startup cache…	4 months ago
po	Update the Russian translate	6 months ago
share	Bump version to 0.3.1 and update changelog	3 months ago
torbrowser_launcher	Actually hide TBL window	4 months ago
.gitignore	ignore source packages that get generated in some dev environments	4 years ago
BUILD.md	Clean up dependencies, and remove requirements.txt because it is out-…	10 months ago
CHANGELOG.md	Bump version to 0.3.1 and update changelog	3 months ago
LICENSE	Update copyright year to 2017	2 years ago
README.md	Add warning about errors to readme, and update screenshot	9 days ago
build_deb.sh	Tweak build files to fix issues in debian building	10 months ago
build_rpm.sh	Tweak build files to fix issues in debian building	10 months ago
makepot.sh	Added a script to generate a pot	2 years ago

Tor Browser for Android (Alpha) - Apps on Google Play - Tor Browser

File Edit View History Bookmarks Tools Help

Tor Browser for Android (

https://play.google.com/store/apps/details?id=org.torproject.torbrowser_alpha&hl=en_US

Google Play

Search

Sign in

Apps

Categories Home Top Charts New Releases

My apps

Shop

Games

Family

Editors' Choice

Account

My subscriptions

Redeem

Buy gift card

My wishlist

My Play activity

Parent Guide

Tor Browser for Android (Alpha)

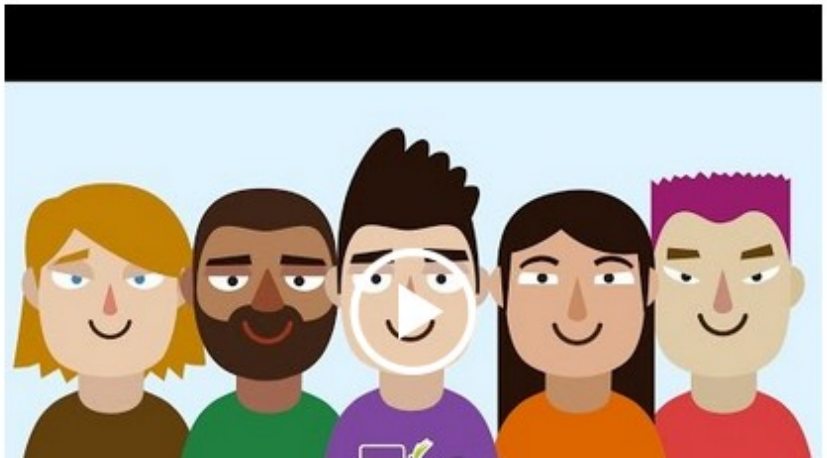
The Tor Project Communication

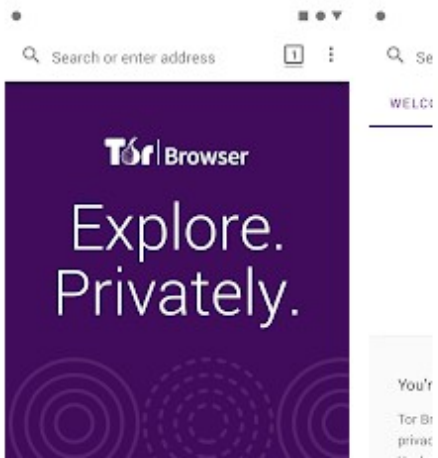
3,421

PEGI 3

Add to Wishlist

Install

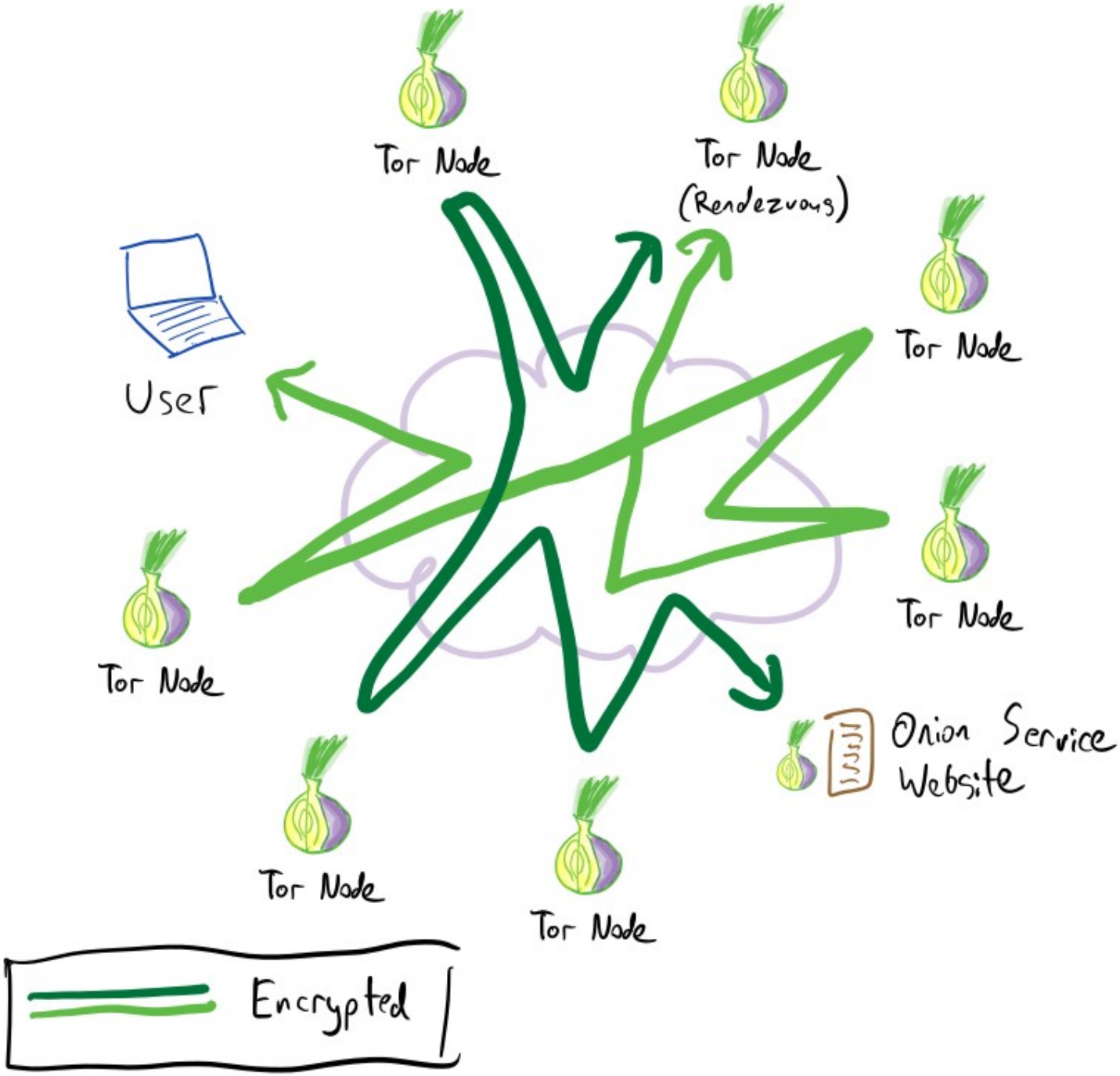




What are onion services?

- Normally, users route traffic through the Tor network to remain anonymous (3 hops)
- With onion services, the server itself routes traffic through the Tor network to remain anonymous (7 hops)
- As long as you can connect to the Tor network, you can run an onion service (bypasses NAT, no port forwarding)
- Use special domain names, where the name itself is a cryptographic fingerprint, so they're self-authenticating:
  - V2 onion service: `http://elx57ue5uyfplgva.onion/`
  - V3 onion service: `http://lldan5gahapx5k7iafb3s4ikijc4ni7gx5iywdflkba5y2ezyg6sjgyd.onion/`

How Onion Services Work



The most popular website on the dark web

Facebook - Log In or Sign Up - Tor Browser

File Edit View History Bookmarks Tools Help

Facebook - Log In or

Facebook, Inc.(US) https://www.facebookcorewwwi.onion

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 14 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 हिन्दी 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

Facebook © 2019

Overview - SecureDrop - Tor Browser

File Edit View History Bookmarks Tools Help

Overview - SecureDrop

https://securedrop.org/overview/

SECUREDROP

Overview List of SecureDrops News Contribute Donate FAQ

Why leading news organizations use SecureDrop to communicate with sources

SecureDrop is an open source whistleblower submission system news organizations can install to safely and anonymously receive documents and tips from sources. It is used at over 50 news organizations worldwide, including *The New York Times, The Washington Post*, *ProPublica*, *The New Yorker*, and *The Intercept*. If you would like to quickly get a feel for the user experience, you can try the demonstration instance on the open web. You can read more about the advantages of the SecureDrop architecture below:

No third parties

Server is completely owned by and sits inside news organization.

Minimizes Metadata

Does not log your IP addresses, browser, or computer.

Encryption

Encrypts your data in transit and at rest.

Protects against hackers

Forces security best practices for journalists & can be used in high-risk environments.

Free Software

OnionShare

Share Files

2 files, 65.8 MiB

instructions.txt 1.7 KiB

leaks 65.8 MiB

Stop sharing

Anyone with this OnionShare address can **download** your files using the **Tor Browser**:

http://bf2o2y5dfycgz3ix.onion/tripping-catcall

Copy Address

Download History 1 0 Clear All

Download Started Nov 25, 01:37PM

17.6 MiB, ETA: 1m47s, 26%

Sharing

A simple onion service

- cd to a director and start a server with:

```
python2 -m SimpleHTTPServer
python3 -m http.server
```

- Edit /etc/tor/torrc and add lines like this:

```
HiddenServiceDir /var/lib/tor/http-onion/
HiddenServicePort 80 127.0.0.1:8000
```

- Restart the tor service, and look at the hostname:

```
sudo systemctl restart tor.service
sudo cat /var/lib/tor/http-onion/hostname
```

Installing a “system tor”

- Linux:
  ```
  sudo apt install tor
  sudo dnf install tor
  ```
- MacOS:
  ```
  brew install tor
  brew services start tor
  ```
- Windows:
  Download “Tor Expert Bundle”, or use Windows 10’s Linux Subsystem. (Or just use Tor from Tor Browser, which is easy.)

Automating anonymous HTTP requests with python

```python
#!/usr/bin/env python3

# Install dependencies:
# pip3 install requests requests[socks]

import requests


# What's my IP and hostname?
r = requests.get("https://ipinfo.io/json")
print("Without Tor:", r.text)

# What's my IP and hostname when I use Tor?
r = requests.get("https://ipinfo.io/json", proxies={
    'http':  'socks5://127.0.0.1:9050',
    'https': 'socks5://127.0.0.1:9050'})
print("With Tor:", r.text)
```

SOCKS proxy, torify

- You can make any program that allows you to configure a SOCKS proxy (OnionShare, Pidgin, HexChat, Twitter on Android, etc.) make connections go over Tor
- You can make command line programs go over Tor with torify, like:

```
torify curl https://check.torproject.org/
```

Tor Isn’t Magic

- Tor doesn’t make you “anonymous”, it **prevents servers on the internet from learning your IP address** – the rest is on you
- Exit nodes can **see your internet traffic**, so use encryption (e.g. HTTPS instead of HTTP)
- Tor is vulnerable to a **global passive adversary**
- Because Tor is meant for low latency activity like web browsing, it’s vulnerable to **traffic correlation attacks**
- If your network is monitored*, the people watching can tell that you’re using Tor, just not what you’re doing (you can hide this using **bridges**)

* All internet traffic is monitored

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to.

a. **Use Tor Browser**

Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser. It is pre-configured to protect your privacy and anonymity on the web as long as you're browsing with Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.

b. **Don't torrent over Tor**

Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor. Even if your torrent application connects only through Tor, you will often send out your real IP address in the tracker GET request, because that's how torrents work. Not only do you deanonymize your torrent traffic and your other simultaneous Tor web traffic this way, you also slow down the entire Tor network for everyone else.

c. **Don't enable or install browser plugins**

Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy.

d. **Use HTTPS versions of websites**

Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, Tor Browser includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include **https://** in the URL, and display the proper expected name for the website. Also see EFF's interactive page explaining how Tor and HTTPS relate.

e. **Don't open documents downloaded through Tor while online**

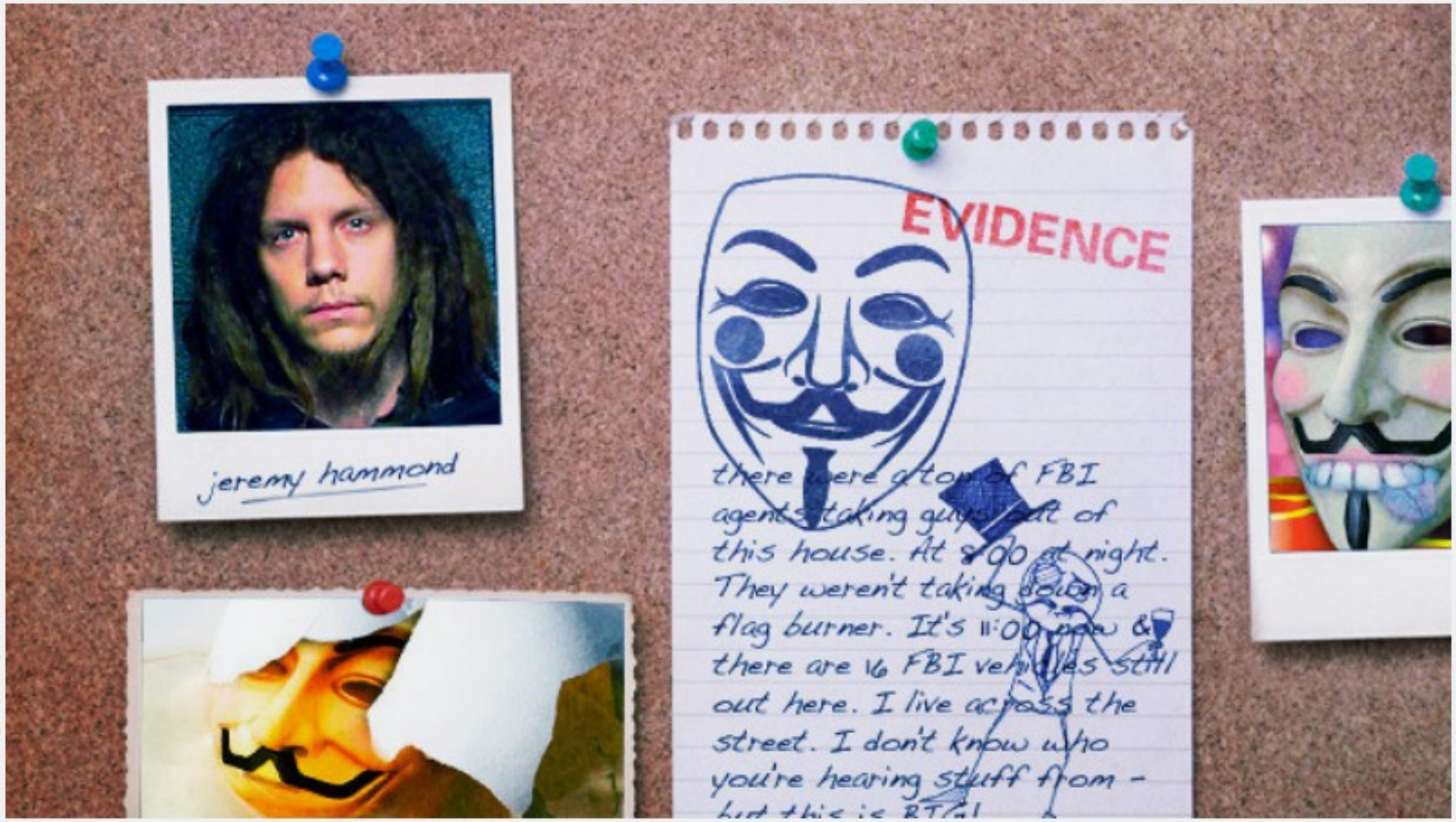
Tor Browser will warn you before automatically opening documents that are handled by external applications. **DO NOT IGNORE THIS WARNING**. You should be very careful when downloading documents via Tor (especially DOC and PDF files, unless you use the PDF viewer that's built into Tor Browser) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.

POLICY —

Stakeout: how the FBI tracked and busted a Chicago Anon

Continuous surveillance, informants, trap-and-trace gear—the FBI spared no ...

NATE ANDERSON - 3/7/2012, 3:30 AM



Photograph by Aurich Lawson

102

"Script kiddie"—no hacker worth his salt wants to hear the term used to describe him. Anyone with modest computer skills can cause modest havoc using other people's code fragments, scanners, and infiltration tools, but this is little more than knowing how to point a gun in the right direction and pull the trigger. It lacks *art*. True hacking requires a deep knowledge of computer

Harvard Student Receives F For Tor Failure While Sending 'Anonymous' Bomb Threat

Runa A. Sandvik Contributor

I cover all things privacy, security and technology.

(Photo credit: joeythibault)

On Tuesday, the FBI filed a criminal complaint against a Harvard University sophomore student for making bomb threats that led school officials to delay some final exams, including his, that had been scheduled for Monday. According to the five-page complaint, the student "took steps to disguise his identity" by using Tor, a software which allows users to browse the web anonymously, and Guerrilla Mail, a service which allows users to create free, temporary email addresses.

Despite 20-year-old Eldo Kim's goal of anonymity, his attempts to mask his identity led authorities right to his front door. Does that mean that Tor failed a user looking to

INTERNET | By Joseph Cox | Nov 7 2016, 7:37pm

Unsealed Court Docs Show FBI Used Malware Like 'A Grenade'

Finally, the warrants and affidavits related to the FBI's use of malware on TorMail have been unsealed.

SHARE TWEET

Image: debradacija/Shutterstock

In 2013, the FBI received permission to hack over 300 specific users of dark web email service TorMail. But now, after the warrants and their applications have finally been unsealed, experts say the agency illegally went further, and hacked perfectly legitimate users of the privacy-focused service.

"That is, while the warrant authorized hacking with a scalpel, the FBI delivered their

OnionScan is a free and open source tool for investigating the Dark Web. Read more about how it works and how to use it on GitHub.

Discovering the Dark Web

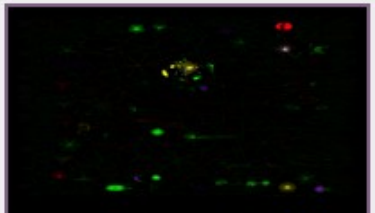
For all the amazing technological innovations in the anonymity and privacy space, there is always a constant threat that has no effective technological patch - human error.

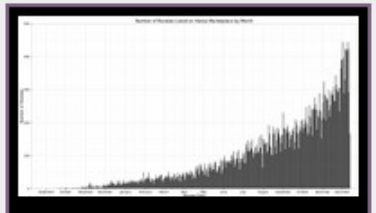
Whether it is operational security leaks or software misconfiguration - most often attacks on anonymity don't come from breaking the underlying systems, but from ourselves.

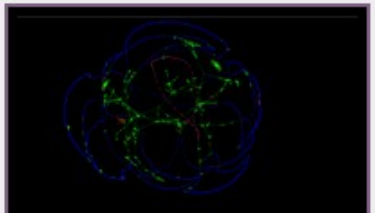
OnionScan has two primary goals:

- We want to help **operators of hidden services find and fix operational security issues with their services**. We want to help them detect misconfigurations and we want to inspire a new generation of anonymity engineering projects to help make the world a more private place.
- Secondly we want to help **researchers and investigators monitor and track Dark Web sites**. In fact we want to make this as easy as possible. Not because we agree with the goals and motives of every investigation force out there - most often we don't. But by making these kinds of investigations easy, we hope to create a powerful incentive for new anonymity technology (see goal #1)

OnionScan Reports







Get OnionScan 0.2

You can find download and installation instructions for OnionScan on our Github

OnionScan is also available on some Linux distributions

Follow Us On Twitter

All of our new reports and releases can be found @OnionScan

In the News

MOTHERBOARD
A Tool to Check If Your Dark Web Site Really Is Anonymous

MOTHERBOARD
Dark Web Drug Dealers are Making Sloppy Mistakes -

naked security by SOPHOS
The Dark Web - Just How Dark is It?

Reporting Bugs

Tails - Privacy for anyone anywhere - Mozilla Firefox

Tails - Privacy for anyone

https://tails.boum.org/index.en.html

Tails

theamnesicincognitolivesystem

search

Tails helps thousands of people stay safe online every day. And it's free.
Donate today to protect and sustain Tails!

$72 880 out of $140 000

1 days remaining

Privacy for anyone anywhere

English DE ES FA FR IT PT

Privacy for anyone anywhere

Tails is a live operating system that you can start on almost any computer from a USB stick or a DVD.

It aims at preserving your **privacy** and **anonymity**, and helps you to:

- **use the Internet anonymously** and **circumvent censorship**;
  all connections to the Internet are forced to go through the Tor network;
- **leave no trace** on the computer you are using unless you ask it explicitly;
- **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

Learn more about Tails.

Install
Tails 3.11
2018-12-11

- About
- Getting started...
- Documentation
- Help & Support
- Contribute
- News

Donate

News

Call for testing: simplified installation method
Posted 2019-01-07

Security

Numerous security holes in Tails 3.10.1
Posted 2018-12-10

Numerous security holes in Tails 3.9.1

Qubes and Whonix

https://youtu.be/f4U8YbXKwog

Qubes OS: The Operating System That Can Protect You Even If You Get Hacked