DARK WEB: How to access safely!

Introduction

In this report we are going to discuss how to access Dark Web safely, things to consider and things to avoid. Here are very beginner friendly instructions on how to setup the Tor and browse for onion links, where the majority of Dark Websites are built on. **This is meant purely for educational purposes. Any misuse of the information provided here will be at your own risk.**

What is dark web?

The dark web is the hidden part of the internet, that you cannot access with normal browsers, where the online activity is intentionally hard to trace. To understand this, think of the internet as 3 layers,

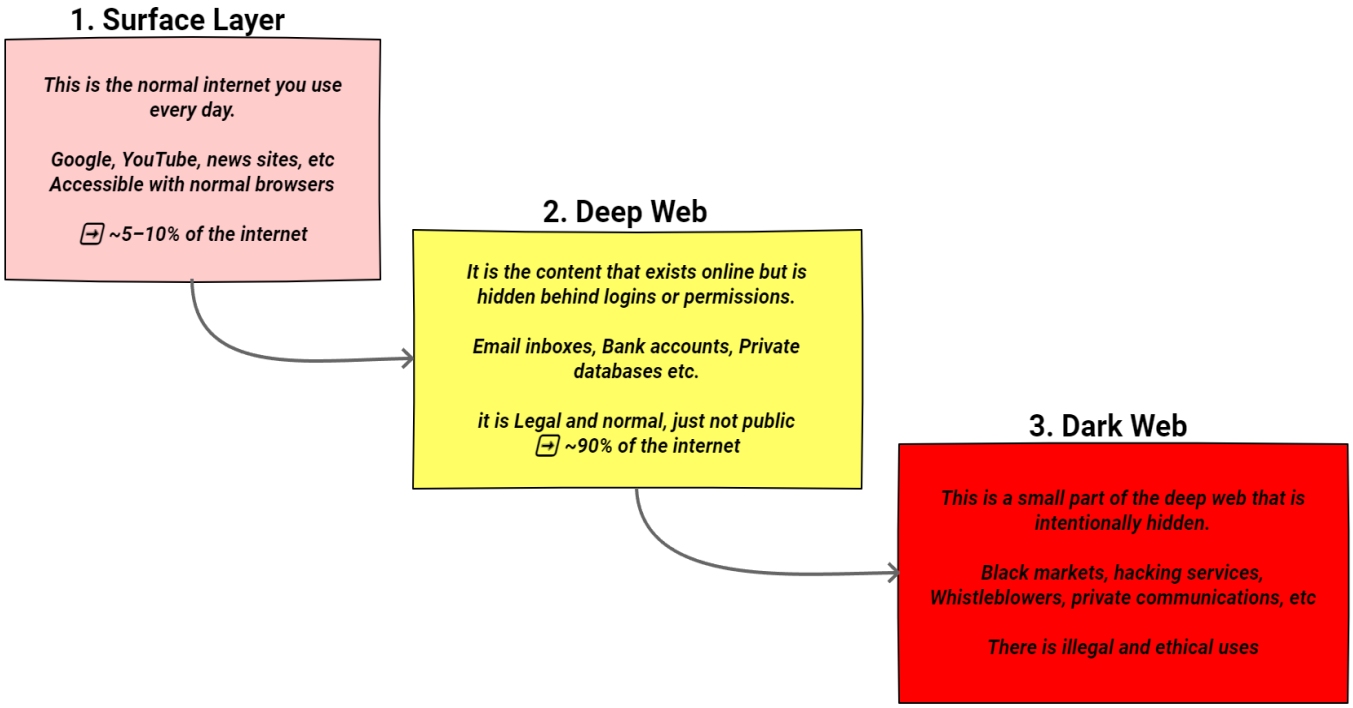

Figure 1

What is the dark web used for?

It has a notorious reputation for stuff like illegal markets for drugs or stolen info, but at the same time it is also a massive lifesaver for privacy. Journalists and whistleblowers use it to

safely transfer information and people in countries with heavy censorship use it to speak freely. That said, for an average person, it's mostly just a wild west where you likely run into scams or viruses if you aren't careful, below are some examples.

Legal and Ethical use

- **Journalists:** Secure Drop (active, used by major news organizations)
- **Whistleblowers:** Edward Snowden (active, currently a Russian citizen and President of the Freedom of the Press Foundation)
- **Activists:** The Tor Project (active, open-source and widely used globally)
- **Privacy-focused communication:** ProtonMail Onion (active, provides secure access in censored areas0

Illegal use

- **Black markets:** Silk Road (shutdown in 2013 by the FBI), Abacus Market (active, currently one of the largest marketplaces)
- **Hacking services:** Genesis Market (shutdown in 2023 by the FBI and Dutch National Police)
- **Document forgery:** LuxSellers (active, various domains seized over time by international law enforcement)
- **Malware distribution:** Russian Market (active, a major hub for selling malware, RDP credentials etc.)

Before we dive into how to connect to dark web, let's go through Tor, which is the tool we will use to access dark web.

What is Tor?

Tor stands for The Onion Route. It is a network and a browser that helps you to stay anonymous online by hiding your identity.

People mainly use Tor through the Tor Browser.

Working of Tor

Tor sends your internet traffic through multiple random servers, called relays.

Think of Tor like sending a secret message through a chain of three different friends who don't know each other. Instead of sending a letter directly to a house (which would reveal your address), you place your message inside three envelopes, one inside the other.

You give the package to the first friend (entry relay).
They remove the outer envelope and can see who you are, but they don't know the destination. They only see instructions to pass the package to Friend B.

Friend B (middle relay) removes the next envelope. They don't know who you are or what the message is. They only know it came from Friend A and must be sent to Friend C.

Friend C (exit relay) removes the final envelope. They can see the destination and the message, but they have no idea who originally sent it, they only know it came from Friend B.

Because each relay only knows one part of the path, no single relay can see both who sent the message and where it's going. This is how Tor keeps users anonymous.

Here, the friends represent Tor relays, and the envelopes represent layers of encryption (onion routing).

The name "Onion" (and the Tor acronym: The Onion Router) was chosen because of how the data is protected by encrypting them in different layers, like peels of an onion.

This technology was created by the U.S. Navy in the 1990s to protect the government intelligence communications before it was released to the public.

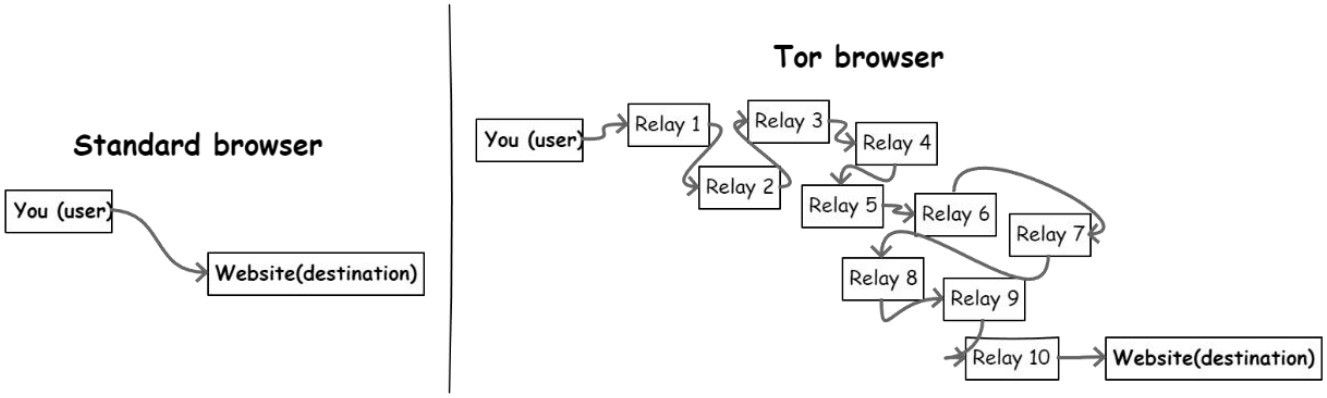

Figure 2

What are Onion websites?

.onion is a special type of address used by Tor, which works only inside Tor, and is not accessible through standard internet. It represents cryptographic identifier, not a name. Standard Domains would use eg: "www.google.com" which are human-readable, and .onion addresses are for instance "ndhd7kss8Jd88nssj4hhfjf8n.onion".

Their key features are;

- Hidden from the regular internet
- Don’t use normal IP
- Location and user identity stays anonymous
- Can only be opened using tor browser
- The connection never leaves the Tor network

Because it provides a high level of anonymity, much of the dark web is made up of .onion websites, which can only be accessed via Tor. Many of these sites are used for illegal activities, though some are also used for privacy.

How to access .onion?

1. Download Tor Browser
   Go to the official Tor Project website to download it.
2. Open Tor browser
   Tor automatically connects you to the Tor network.
   Think of it like entering secret tunnel wearing a mask.
3. Use .onion links
   .onion addresses are the URLs of the dark web sites.
   They are not easy to find, so you usually need to spend a lot of time browsing to get a working .onion link.
4. Browse inside Tor
   Once connected, you can visit .onion sites just like normal websites, since connection is passed through many relays for anonymity, it can be slower than usual, so patience is key here.

Safety Tips

- Don’t download files from untrusted sites
- Do not share personal information.
- Stick to legal websites unless you know exactly what you are doing
- Use VPN for extra safety (recommended)

Using VPN with Tor

Even though Tor is designed for anonymity, using aa VPN can add an extra layer of security. A VPN can hide the fact that you ae using Tor from your Internet Service Provider (ISP), encrypt your internet traffic before it enters Tor, and sometimes helps to get over Tor restrictions in certain countries. Below are the two ways to use VPN with Tor,

1. **VPN over Tor (Tor first, then VPN)**
   Here you first connect to Tor, then you traffic goes through the VPN.
   Pros:
   - Your ISP cannot see what websites you visit on Tor
   - VPN only sees traffic coming from Tor, your identity is hidden from the VPN.

   Cons:

   - VPN provider could see you are using Tor
   - Slower speed due to multiple layers of routing.

2. **Tor over VPN (VPN first, then Tor) RECOMMENDED**
   You first connect to a VPN, then Tor.
   Pros:
   - ISP cannot see you are using Tor
   - Hides your real IP from the Tor entry nodes

   Cons:

   - You must trust the VPN provider with your real IP
     Ensure that VPN has no logs policy, so that they don't track your online activities.
   - Slightly more complex setup

Conclusion

To conclude, Dark Web is buried beneath all the internet that is available on the surface. You need specialized browsers to access them, and we cannot use regular browsers. There are legal and illegal things happening in Dark Web and in most of the countries browsing in Tor has no restriction, but make sure you use it for legal and ethical purposes, unless you know exactly what you are doing.