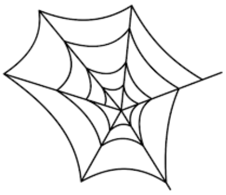


Dark Web

The article is designed for students and anyone else who is interested in Dark Web

Paata Gogishvili

Doctor of Informatics, Associate Professor at Ilia State University

paatagog@gmail.com, paata.gogishvili@iliauni.edu.ge

www.max.ge

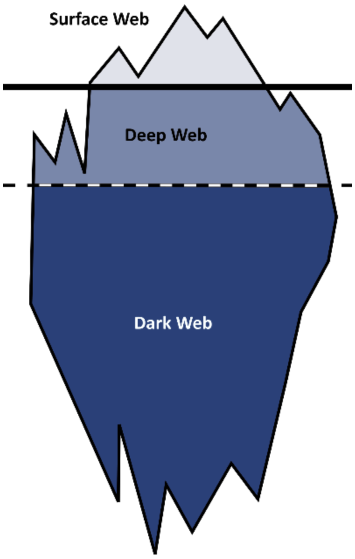
Definition

The internet is like an iceberg: what we see on the surface, known as the "surface web," is just the tip of the iceberg. Beneath the surface lies the vast "deep web," where most online activities occur without public indexing. Deeper still, we encounter the enigmatic "dark web," a realm often shrouded in mystery, intrigue, and even fear.

Remember that the dark web is not inherently evil, just as the surface web isn't inherently good. It's a tool, and like any tool, its ethical use depends on how it's wielded. Respect the privacy and anonymity of others, avoid harmful content, and always follow ethical guidelines.

Surface Web

This is the internet we use every day. It consists of websites indexed by search engines like Google or Bing. You access these sites using standard web browsers, and their content is publicly available. Information, businesses, social media, news, and everything in between reside here.



Deep Web

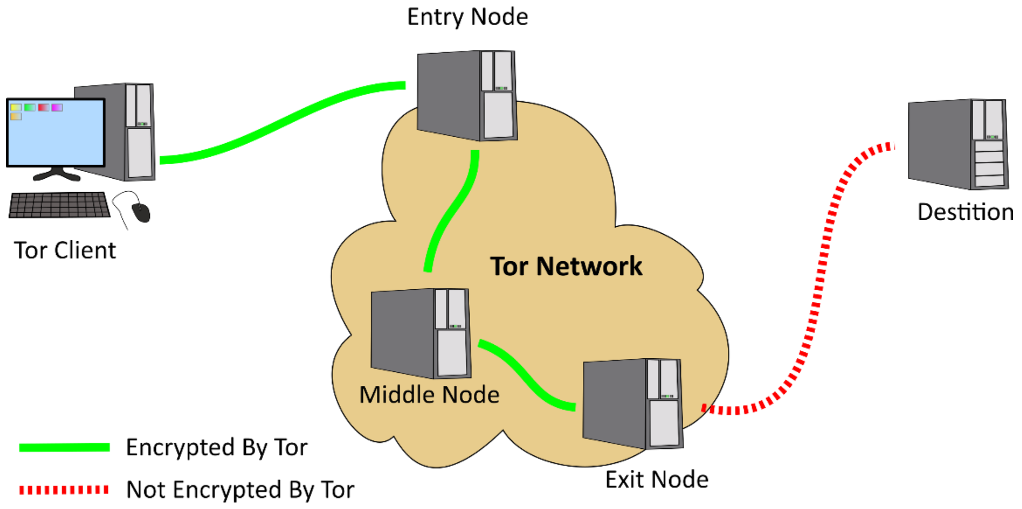
Below the surface web is the deep web. It includes databases, private networks, and content behind paywalls, all inaccessible to search engines. Your email inbox, online banking, and academic databases are part of the deep web. These resources require login credentials or special permissions to access.

Dark Web

The dark web, on the other hand, is intentionally hidden and can only be accessed using specialized software, most notably Tor (The Onion Router). It's a place where anonymity is prized, and websites often have obscure domain extensions like "`.onion`". While it's a space where privacy can be maintained, it also has a darker side, hosting marketplaces for illegal goods, forums for criminal activity, and other hidden corners of the internet.

Underline Mechanism of the Dark Web

At the heart of the dark web is the Tor network, which stands for "The Onion Router." Tor is a free, open-source software that enables anonymous communication over the internet. It achieves this by routing data through a network of volunteer-operated servers, or nodes, before it reaches its final destination.



When a user wants to access a website or service on the dark web, their traffic is encrypted and sent through a series of Tor nodes. These nodes are like layers of an onion, hence the name "onion routing." Each node in the chain peels back one layer of encryption to reveal the next destination, making it extremely difficult to trace the original source. The nodes of the network can be divided into three categories: Entry nodes, Middle Nodes and the Exit Nodes.

Entry Node

The journey begins at an entry node (also called a guard node). This is the first node in the chain. It knows your IP address but doesn't know what you're doing on the internet because your data is encrypted. The entry node passes your data to the next node in the chain.

Middle Node

Next, your data is sent through one or more middle nodes. These nodes only know the IP address of the previous and next nodes in the chain. They have no knowledge of the original source or the final destination. Each middle node decrypts a layer of encryption and forwards the data to the next node.

Exit Node

Finally, your data reaches an exit node. The exit node decrypts the last layer of encryption and sends your request to the destination website or service on the dark web. Importantly, the exit node's IP address is the one visible to the website or service you're accessing, not your own. This provides the anonymity crucial to dark web users.

Websites on the dark web often use a special domain extension called "`.onion`". These websites can only be accessed through the Tor network. They are designed to provide anonymity to both the site's host and its visitors. When you access a `.onion` site, your request is routed through the Tor network in the same manner as explained above.

The combination of multiple layers of encryption and routing through a network of nodes ensures a high degree of anonymity and privacy for users of the Tor network. It makes it exceedingly difficult for anyone, including government agencies and cybercriminals, to trace the origin of data or identify the user.

However, it's essential to note that while Tor provides strong anonymity, it doesn't guarantee absolute security. Users must still practice good cybersecurity hygiene and be cautious about sharing personal information or engaging in illegal activities on the dark web.

Some Resources of The Dark Web

DuckDuckGo

DuckDuckGo is a privacy-focused search engine that emphasizes user privacy, data security, and anonymity. Note that it searches web surface sites, not the `.onion` ones.

https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

Ahmia

Ahima is the search engine for the `.onion` sites.

http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

The Hidden Wiki

The Hidden Wiki is a dark web site that serves as a directory of links to various websites and resources. It includes links to blogs, information repositories, technical guides, and more. It's a starting point for users looking to explore the diverse content available on the dark web.

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion

Dark Net Forum

Dark Net Forum is a dark web forum where users can discuss various topics anonymously. It functions similarly to surface web forums but with an emphasis on privacy and anonymity. Users might engage in discussions related to technology, cybersecurity, privacy tools, and even political activism

http://3otgxq7d33rwspxfquwkqlp7r4yoicofniypk7hcxxqefrwhptqp7zad.onion

Market Place

This is an example of a dark web marketplace. While it hosts legal products like digital art and software, it also contains listings for illegal items such as drugs and hacking services. Transactions typically occur using cryptocurrencies like Bitcoin.

http://shoprypxphsufyldigdn34kbjbsnjnrmv2z34yc5al5lkmveqcbex2qd.onion

The Role of Cryptocurrencies in Dark Web Transactions

The dark web has gained notoriety for various illicit activities, including the buying and selling of illegal goods and services. Cryptocurrencies, particularly Bitcoin, play a pivotal role in facilitating transactions within this secretive digital realm.

Cryptocurrencies offer a level of pseudonymity and privacy that traditional financial systems cannot match. Bitcoin transactions are recorded on a public ledger called the blockchain, but they do not inherently reveal the identity of the parties involved. Instead, transactions are associated with alphanumeric addresses, providing a degree of anonymity. Dark web users leverage this feature to shield their identities when conducting transactions.

Users of the Cryptocurrencies are trying to find the way of escaping traditional financial institutions and making cross-border transactions.

It's worth mentioning that Tor and blockchain are both decentralized systems with similar goals: ensuring confidentiality and enhancing user freedom.

The Tor network was invented before blockchain technology. It was developed by computer scientists Roger Dingledine, Nick Mathewson, and Paul Syverson in the late 1990s. It was first deployed and made publicly available in 2002.

Blockchain technology, which underlies cryptocurrencies like Bitcoin, was invented by an individual or group using the pseudonym Satoshi Nakamoto. The Bitcoin whitepaper, titled "Bitcoin: A Peer-to-Peer Electronic Cash System," was published in October 2008. The Bitcoin network itself was launched in January 2009.

Creating and hosting `.onion` website on the Tor network

It is easy to create and host the website of the Tor Network.

Install the tor at first

```
sudo apt install tor
```

Install your web server

```
sudo apt-get install apache2
```

Edit the `/var/www/html/index.html`, place the following (or any other) content

```
<!DOCTYPE html>
<html>
<head>
    <title>Hello Tor</title>
</head>
<body>
    <h1>Hello, Tor World!</h1>
</body>
</html>
```

Edit the Tor configuration file `/etc/tor/torrc`. Add (or uncomment) the following lines

```
HiddenServiceDir /var/lib/tor/mywebsite/
HiddenServicePort 80 127.0.0.1:80
```

This configuration tells Tor to create a hidden service directory at `/var/lib/tor/mywebsite/` and forward incoming requests on port 80 to your web server running on 127.0.0.1 (localhost).

Restart the Tor service to apply the configuration changes using the following command

```
sudo systemctl restart tor
```

Retrieve your .onion address from the hidden service directory

```
sudo cat /var/lib/tor/mywebsite/hostname
```

This command will display your `.onion` address, which will look something like a random string of characters followed by "`.onion`".

Your `.onion` website is created and is hosted on the Tor Network.

Open the Tor Browser on your computer and enter your `.onion` address in the Tor Browser's address bar in order to access your `.onion` website.

You can always delete your web site when needed.

Delete the HTML file for your website using the following command

```
sudo rm /var/www/html/index.html
```

Remove the Tor hidden service directory associated with your website:

```
sudo rm -r /var/lib/tor/mywebsite/
```

Replace "mywebsite" with the directory name you used in your Tor configuration

Stop and disable the Tor Service

```
sudo systemctl stop tor
sudo systemctl disable tor
```

The first command stops the service. The second command prevents the Tor service from starting at boot time. If you wish to re-enable it later, you can use `sudo systemctl enable tor`.

Stop and disable the Apache Web Server

```
sudo systemctl stop apache2
sudo systemctl disable apache2
```

The first command stops the service. The second command disables the Apache service from starting at boot. You can re-enable it later using `sudo systemctl enable apache2`.