 **National College of Computer Studies**

**Paknajol, Kathmandu**

**Report on**

**Dark Web**

**Submitted by:                                                Submitted to:**

Swarup Dahal Dadhi Ram Ghimire

Program: BSc.CSIT 1st Semester           TU Lecturer

Roll. No: 22

Email: [swarupdahal17@gmail.com](mailto:samriddhishakya617@gmail.com)**Abstract:**

The dark web is the part of the World Wide Web that is only accessible utilizing special software, allowing users and website operators to remain anonymous or untraceable. The dark web is one of the web browsing platforms in which important data, illegal data, and records are kept secretly. The dark web is part of the deep web. The dark web cannot be easily browsed by a normal user. This report provides the necessary information about the dark web. Normally, we can say that the dark web is a kind of a browsing platform where both legal and illegal work is done by users. It talks about how the dark web was first introduced and used. The dark web is usually browsed by hackers, military defense sectors, etc to keep the information private and secure. Normal users like us can`t browse the dark web easily. When a user enters the dark web they can observe and browse many sites which are not browsed by the surface web. The dark web can be browsed through the browser name TOR browser. Anonymity, privacy, and the possibility of non-detection are three factors that are provided by TOR and I2p. In this article, we're going to analyze and produce findings on the effect of the Dark Web on various realms of society. There are many dark web users in this world. On the dark web, the name of the user is not confirmed or identified. The TOR browser is committed to carrying out secret tasks and private works. Given the number of daily anonymous users of the Dark Web (TOR) in the whole world for a while. The influence of hidden services websites is shown and results are gathered from Ahimia and Onion City Dark Web's search engines. In such networks, users are calculated through the client request of directories (by TOR metrics) and the relay list is updated. Indirectly, the number of users is calculated for the anonymous networks.

Keywords: Dark Web, Tor, I2P, Anonymity

Table of Contents

[**1.** **Introduction and History:** 1](#_Toc119341633)

[**2.** **How access Dark Web?** 2](#_Toc119341634)

[3. **TOR browser**: 2](#_Toc119341635)

[**4.** **Invisible Internet Project (I2P):** 2](#_Toc119341636)

[**5.** **Uses of the Dark Web:** 3](#_Toc119341637)

[**6.** **Applications of Dark Web:** 4](#_Toc119341638)

[A. Dark Web in hacking: 4](#_Toc119341639)

[B. Dark web in military defense: 5](#_Toc119341640)

[C. Dark web on trading: 5](#_Toc119341641)

[**7.** **Security Issue on Dark Web:** 6](#_Toc119341642)

[a) Virus: 6](#_Toc119341643)

[b) Worms: 6](#_Toc119341644)

[c) Hacker: 7](#_Toc119341645)

[**8.** **Conclusion:** 8](#_Toc119341646)

[Figure 1: Parts of Web 1](file:///C:\Users\User\Desktop\National%20College%20of%20Computer%20Studies.docx#_Toc108359780)

[Figure 2: Tor browser 2](#_Toc108359781)

[Figure 3: I2P browser 2](#_Toc108359782)

[Figure 4: Uses area of dark web 3](#_Toc108359783)

[Figure 5: Hacker 4](#_Toc108359784)

[Figure 6: Military defense unit 5](#_Toc108359785)

[Figure 7: Bitcoin 5](#_Toc108359786)

[Figure 8: Virus 6](#_Toc108359787)

[Figure 9: Worms 6](#_Toc108359788)

[Figure 10: White hat hacker 7](#_Toc108359789)

[Figure 11: Grey hat hacker 7](#_Toc108359790)

Figure 12: Black Hat Hacker 8

# **Introduction and History:**

The internet requires numerous networks and vast infrastructure. (Gehl, 2016) We know at a time millions of computers can be linked by establishing a network in which each computer can interact with other computers as long as it is linked to the Internet. One of the components of the internet is Dark Web, which applies to a subset with its contents where it is used for various technical purposes [1]. The dark web contains information on private networks and agencies. Dark Web content is intentionally hidden and cannot be accessed by the standard web browser. The owners of the Dark Web are anonymous and secret. Dark Web is accessible to exchange low-risk and undetected information. The TOR browser project was initiated in 2002 by the US Naval Laboratory to allow anonymous online communication. Invisible Internet Project (I2P) is another network on the Web with data at its edge that is used for secure communication, information, encryption, etc. (Hurlburt, 2017) TOR allows user to channel their traffic via "server machines" in such a manner that traffic not tracked back to the original users and their identity is concealed. TOR has built "relays" on computers that hold information via tunnels all around the world. Dark Web can be accomplished utilizing open and cooperative nodes of other network communities (Tor or I2P). (Harrison, 2016) Dark Web is any Internet content that cannot or is not indexed by search engines such as Google [2]. Relevant applications like TOR can give access to the Dark Web. Most of the collective interest in the Dark Web rests in the practices that take place inside the dark net.

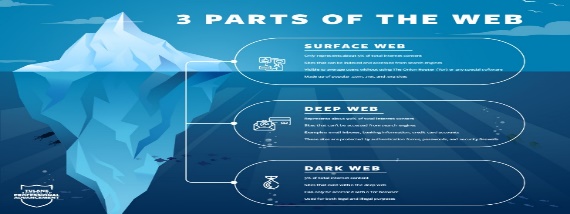


Figure 1: Parts Web

# **How access Dark Web?**

To access the dark web, you need to have a Tor browser on your system. First, download the tor and then install it on your system. Open the installed Tor browser and you can browse the dark web using Tor browser. If you want to access dark web sites you may need onion link on your Tor browser. And you have to make sure your security level is strong and your privacy are secured while browsing dark web. You also can use different strong VPN service to make your security level strong.

# **TOR browser**:

The Tor browsing is usually known as onion routing. The Tor Browser is a web browser designed for anonymous web surfing and protection against traffic analysis. Although Tor is even associated with the dark net and criminal activities. Tor browser gives access to browsing the dark web. Tor is the most used browser among the dark web browsers. The TOR browser project was initiated in 2002 by the US Naval Laboratory to allow anonymous online communication. [3]

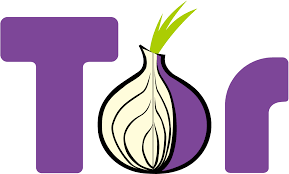


Figure 2: Tor browser

# **Invisible Internet Project (I2P):**

I2P is an anonymous network layer that allows for peer-to-peer communication. Anonymous connections are achieved by encrypting the user's traffic (by using end-to-end encryption) and sending it through a volunteer-run network of roughly 55,000 computers distributed around the world. Given the high number of the possible path the traffic can transit, a third party watching a full connection is unlikely. The software that implements this layer is called the "I2P router", and a computer I2P is called an "I2P node". I2P is free and open source and is published under multiple licenses. [5]



Figure 3: I2P browser

# **Uses of the Dark Web:**

There are enormous uses of the dark web. As we all know the dark web can be used for both legal and illegal purposes. Like dark web be used for illegal hacking. There are so many people who want to keep their data hidden from the government that they use the dark web to keep them secret. Normally, hackers use the dark web to keep their identities hidden. On the dark web selling of weapons, drugs, and different other illegal activities are done. Military defense units and different big organizations use the dark web to keep their data and information safe. On the dark web, a person can hire a killer if he wants to kill someone. But on the other side of the coin, people who want to plot an assassination versus a high-profile target will want a method that is guaranteed to be untraceable. Certain illicit activities, such as the selling of papers such as passports and credit cards, would also include a network that ensures anonymity. The same may be done to people who have leaked sensitive information from other individuals, such as emails and contact numbers. Normally on the dark web, we cannot trace users' location because their information is kept anonymous. To carry out all these activities payment is done through Bitcoin because Bitcoin can't be traced. [5]



Figure 4: Uses area of the dark web

# **Applications of Dark Web:**

## Dark Web in hacking:

In hacking dark web is used to make the identity of the user anonymous so that other people cannot locate the area or IP address of the hacker. There are different hackers available on the dark web like white hat hackers, grey hat hackers, and black hat hackers. Generally, hackers use the dark web to retrieve the private information of different organizations or persons. There are different hackers available on the dark web like malware, crypter, etc. The numbers of hackers on the dark web are numerous. By using the dark web hackers can make their identity hidden and they can access many different IP addresses so that it will be difficult for someone to locate them. [6]



Figure 5: Hacker

## Dark web in military defense:

The military (US Navy) created the Dark Web and TOR in the mid-1990s to create a technology that allowed intelligence operatives to exchange information completely, and anonymously. They called the project TOR which means "The Onion Router". Essentially, they created this project on an Internet that was reserved for military use in the same way the Internet was used for military communication in the beginning, as a government communication. As part of their strategy for secrecy, they released TOR into the public domain for anyone to use. Since 2004, TOR has gone Open Source and is used widely used in the public domain. TOR keeps your anonymity by bouncing your Internet traffic across various network relays around the world. Your communication CAN go from the USA to South Africa, to Hong Kong, to Germany, then back to the USA in one conversation, but your communication may seem normal to you. However, your traffic is bouncing all over the world. During this route, your available location and your name have dropped off a bit. Your communication may not be complete also. Also, the person with whom you may be talking is anonymous and is always kept secret, in the same way as you are anonymous. This is why we say, you don't know who you are dealing with. The person you talk with on the dark web, although seems normal in a conversation, may have surprises for you. Beware of the worst that can happen. Guard your computer. Even that may not be enough. [7]



Figure 6: Military defense unit

## Dark web on trading:

The dark web on trading is known as the dark net market which is the commercial website in a dark web that is browsed through the Tor browser. They function primarily as a black market, selling or brokering transactions involving drugs, cyber arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illegal goods as well as the sale of illegal products. To carry out all these activities on the dark web payment is done through crypto currency or bitcoin or monero payment with escrow service, and an eBay-like vendor feedback system. [8]



Figure 7: Bitcoin

# **Security Issue on Dark Web:**

There are lots of security issues on the dark web such as [9]

### Virus:

A Virus is a program that is loaded into your machine without your knowledge and runs against your wishes. They are computer programs that bind themselves to or corrupt the machine or files which appear to circulate to other machines on the network by clicking on them, by fax, by mobile devices, etc. They interrupt the operation of the machine and affect the data stored either by changing it or by deleting it entirely. Definition of viruses: (1) Melissa, (2) Sasser, (3) Zeus, (4) Conficker, (5) Stuxnet, (6) Mydoom, (7) Red Code.



Figure 8: Virus

### Worms:

Worms, unlike viruses, do not require a host to cling to. They're only replicating until they've used up all the resources left on the machine. The word "worm" is often used to mean "self-replicating" malware (Malicious software). It has some free memory of drives or other computers. Examples of heat: (1) Badtrans, (2) Bagle, (3) Gun, (4) ExploreZip, (5) Kak worm, (6) Netsky, (7) SQL Slamme.



Figure 9: Worms

### Hacker:

A rising hacker is a person who breaks into computers, usually by obtaining access to administrative controls. Types of hackers are:

#### White hat hacker:

A white hat hacker is an information security expert who hacks into secure systems and networks to check and determine their protection. White hat hackers use their expertise to boost security by revealing bugs to malicious hackers (known as black hat hackers) who can identify and manipulate them. While the methods used are similar, if not equivalent, to those used, malicious hackers, white hat hackers, have permission to recruit them against the company that recruited them.



Figure 10: White hat hacker

#### Grey Hat Hacker:

The word "white hat" or "blue hat" applies to a computer hacker or information security specialist who can often break the law or traditional ethical norms, but who has no criminal intent characteristic of a black hat hacker.



Figure 11: Grey hat hacker

#### Black Hat Hacker

A black hat hacker is a person with advanced computer skills whose aim is to break or circumvent Internet security. Black hat hackers are also known as crackers or dark-sided hackers. The general opinion is that while hackers are constructing stuff are smashing things.



Figure 12: Black Hat Hacker

# **Conclusion:**

Dark Web networks such as TOR have created a wide variety of ways for criminal individuals to trade legitimate and illicit "goods" anonymously. Dark Web is a growing commodity, especially in the field of illegal resources and activities. Protection processes should be proactive in resolving these problems and taking steps to remove them. This paper explores the effect of the Dark Web, the secrecy and confidentiality of the Dark Web, and the findings show anonymous users daily the amount of this Internet section for the world as a whole, and the effect of secret resources websites on the Dark Web. [10]

Reference:

[1]Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the Dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*. <https://doi.org/10.1002/asi.20838>

[2] Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media and Society*. <https://doi.org/10.1177/1461444814554900>

[3]"TOR browser" retrieved from

<https://www.techtarget.com/whatis/definition/TOR-third-generation-onion-routing#:~:text=The%20Tor%20(the%20onion%20routing,and%20protection%20against%20traffic%20analysis.>

[4]"I2P" retrieved from

<https://www.techtarget.com/whatis/definition/TOR-third-generation-onion-routing#:~:text=The%20Tor%20(the%20onion%20routing,and%20protection%20against%20traffic%20analysis.>

[5]"Uses of dark web' retrieved from

<https://doi.org/10.1002/asi.20838>

[6]"Dark web on hacking" retrieved from

<https://resources.infosecinstitute.com/topic/hacking-communities-in-the-deep-web/>

[7] "Dark web on military defense" retrieved from

<https://www.quora.com/>

[8] "Dark web on trading" retrieved from

<https://en.wikipedia.org/wiki/>

[9]"Security Issue on dark web" retrieved from

<http://www.jetir.org>

[10]"Conclusion" were retrieved from

<http://www.jetir.org>