iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46577

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Dark Web: The Hub of Crime

Srinjoy Saha[1], Sanhita Kar[2], Chayantika Roy[3], Sneha Nej[4], Meghna Das[5], Soumita Mullick[6], Debrupa Pal[7]
[1, 2, 3, 4, 5, 6]*BCA IInd year, Department of Computer Application, Narula Institute of Technology, Kolkata, West Bengal, India*
[7]*Assistant Professor, Department of Computer Application, Narula Institute of Technology, Kolkata, West Bengal, India*

Abstract: ***Now days Internet plays a significant role in our daily life. It's become an essential part of all daily lifestyle. Dark Web is like an untraceable secret layer of the Internet which basically used to store and access the sensitive and confidential data. But we can see the huge misuse of this platform for conducting the criminal and illegal activities in a hidden way. In this paper, we are going to discuss about the overview of dark web and many browsers those are used to access dark web. We also discuss about the methods used in Dark web for anonymity and confidentiality.***
Here some interesting facts are also discussed about dark web and the different types of crimes to create awareness about this type of activities and the preventive action for these activities.
Keywords: Dark Web, Tor Browser, Onion Routing, Silk Road, Red Room.

I. INTRODUCTION

In this technological world, web security has become a vital area of concern as most of users visit online for full fill their needs. As the Internet continued to grow in the middle of 1990s it had come to transform so many things. The biggest change is instant communication. If you have an Internet connection, you can talk to anyone instantly.
But the Internet was not structured with elements like privacy, security and anonymity in mind, it is the main concern. So, every single thing can be tracked. But some people are very worried about their privacy and security. So, the dangerous, colossal secret od internet is dark web.
Today's number one source for stolen information and criminal services is as interesting a talking point as it is dangerous to browse. Whether we are talking about the sensitive personal information stolen in the Equifax breach, personal healthcare information stolen in the Anthem breach and the credit/debit card information stolen in the argot breach, they all have at least one thing in common: this stolen information eventually makes its way to the dark web to be sold and purchased.
Dark web cannot be accessed by regular web browsers like google chrome, internet explorer or Mozilla Firefox. The most common tool for accessing the dark web remains a browser called Tor, or "The Onion Router," which was created by the military to protect oversea communications.

II. STRUCTURE OF THE INTERNET

There are three parts that consists of world wide web (www) as shown in Figure 1.

1) *Surface Web:* The first part is surface web, the surface web which is also known as the visible web, index-able web, or clearnet is content on the world wide web. The surface web is what users' access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft's Internet Explorer or Edge, and Google Chrome [1]. Some of the examples of surface web are Google or Yahoo. Facebook, YouTube, Wikipedia, Regular Blogging Websites, and basically everything that we can see on any search engine's result page.
2) *Deep Web:* The second part is deep web, the deep web which is also called as hidden web or invisible web, the deep web is different from the surface web. The deep web helps people to maintain privacy and freely express their views. Privacy is essential for many innocent people terrorized by stalkers and other criminals. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity [2]. Example of Deep Web includes email messages, chat messages, private content on social media sites, electronic bank statements, electronic health records (EHR) and other content that is accessible one way or another over the internet.

.

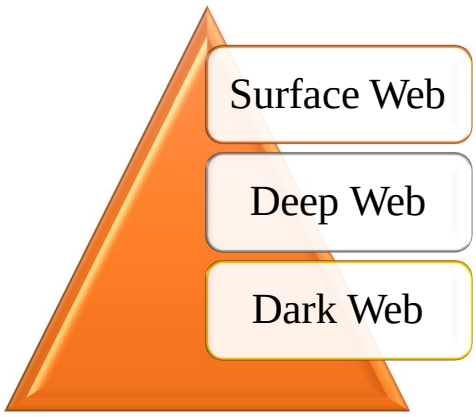


Figure 1: Structure of Internet

3) *Dark Web:* The final part is Dark Web, the dark web is known to have begun in 2000 with the release of Free net, the thesis project of University of Edinburgh student Ian Clarke, who set out to create a "Distributed Decentralized Information Storage and Retrieval System." Clarke aimed to create a new way to anonymously communicate and share files online [3]. The dark web is a network that constitutes a part of the global Internet platform not indexed by search engines, which requires some form of authentication to gain access. Such authorization may require using specific software, such as proxy software, to gain access to the dark web websites. Some of the examples of dark web include human trafficking, drug trade, weapons dealing to name a few. There are various reasons to stay off the dark web. However, at the same time, it's a place worth visiting too. The dark web isn't for everyone, but some of it is worth exploring. Some examples for dark web websites include Tor, DuckDuckGo, ProPublica, SecureDrop, Ahmia etc [4][5].

III. HOW TO ACCESS DARK WEB

There is no concept on the internet that is more infamous than the dark web. There is no saying how vast the dark web is, but one thing for sure, the clear web and deep web dwindle in comparison. To dive down deep into the dark web, onion router is used, better known as Tor as shown in Figure 2. While this is not the only option, it's probably the most convenient and arguably, the safer option. Apart from the Tor browser, there are many browsers that we can use for accessing the dark web like – Freenet, Whonix, Subgraph OS, I2P (Invisible Internet Project) etc. But this paper is focused on Tor[6][7].

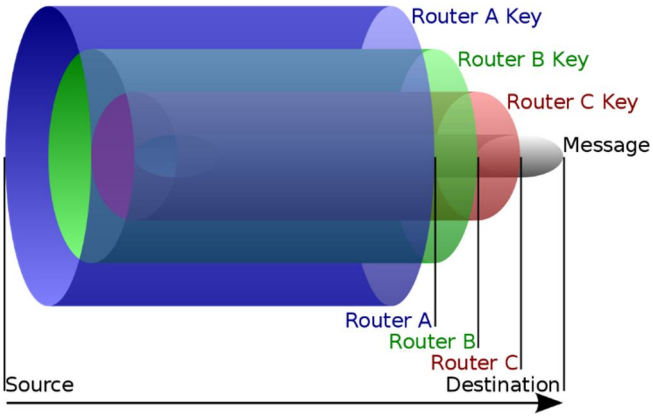


Figure 2: Diagram of Onion Routing

Now, the easiest way to use Tor is to get a Tor browser, which functions as any other browser would. Tor helps us to reroute our web requests through a series of proxy nodes, chosen at random and located anywhere in the world. That way your connection won't be traced back to you [8].

A. Features of Tor Browser

1) It's a combination of Firefox browser and Tor project.
2) Tor browser is an open-source software.
3) Automatic data decryption at client side.
4) Overlay network is used to direct the internet traffic.

B. Advantages of using Tor Browser

1) Protects the privacy of the users by hiding their IP addresses.
2) The websites we open in this browser is secured and encrypted.
3) Anti-spy protection is one of the benefits of using Tor, it prevents others from tracking the websites we visit.

C. Disadvantages of using Tor Browser:

1) Low latency is a major problem of using Tor browser.
2) We can't download and upload large files through this browser.
3) The exit node has the data regarding the websites that are visited, that's why security is an issue of this browser.

IV. METHODS USED IN DARK WEB

The dark web can be quite a dangerous place if the right precautions are not taken. There are the crucial steps we need to take if we want to know how to access the dark web in a safe and anonymous way. However, we should keep in mind that things change quickly and hackers get smarter every day.

1) *Always Use a VPN to Access the Dark Web:* Even if we use the Tor browser, our traffic can still be traced back to us by anyone with sufficient time, resources, and know-how. In fact, the Tor browser was found to have a vulnerability in 2018 that in some instances leaked real IP addresses. Therefore, if we want to use Tor privately, we can use either a VPN or Tor Bridges (Tor nodes that are not publicly indexed) to connecting to the dark web. When using a VPN for the dark web, our ISP will not be able to see that we are connected to a Tor node, only an encrypted tunnel to a VPN server.
2) *Download the Tor Browser from the Official Website:* Tor might have had its security problems in the past, but it's still the most popular way to get on the dark web. The Tor browser is an interesting target for hackers and government agencies. Fake versions of the Tor browser have been created to either breach users before they even access the dark web or monitor the behavior of a user while on the dark web. Because of its market-leading position and the nature of the content which we can access when using it, it should come as no surprise to learn that there are a lot of bad actors out there. These people try to spoof the app and make you download a compromised version instead. Therefore, we should never download the Tor browser from any source other than the official website. It can be found at torproject.org. The browser is free to download and use.
3) *Take Security Precautions:* The dark web is a popular hangout for hackers, cybercriminals, malware creators, and other unsavory types that we really don't want anywhere near our machine.

Therefore, Before open the Tor browser, we should:

- Have a reputable and fully updated antivirus program installed on device.
- Close all non-essential apps on our machine, password managers.
- Turn off location on our device. Our location can be found through our IP-address as well as our device itself.
- Cover webcam with a piece of paper. It is shockingly easy to gain access to our webcam, even without noticing.

4) *Know Where You're Going:* It can be hard to navigate the dark web. While access the dark web, we won't have the luxury of Google neatly indexing search results for us to browse. As a result, it can be hard to find what we're looking for; we could easily stumble into someplace, we really don't want to be. The dark web itself also has plenty of dark web site directories. It isn't wise to randomly click around and visit websites. The dark web contains many dangers we should definitely avoid. In order to get some sense of direction on the dark web, we can use a couple of directory sites to guide us. One of the most common places that many first-time users visit, is "The Hidden Wiki ".
5) *Use Cryptocurrency for All Your Transactions:* In the dark web, anonymity plays a big role. This is also the case with online payments, everyone uses cryptocurrency. If we purchase something through our bank, credit card, PayPal, or another regular payment method, companies and governments will know. With cryptocurrencies, this isn't the case: both buyer and seller remain much more anonymous. If our encounter someone on the dark web who wants to arrange a transaction through a regular bank, we're probably dealing with a scammer hacker, or spy.

6) *Close Everything:* All of the browser windows and any other related content that may be connected need to be closed properly. Shut down the whole Tor browser. If we've used TAILS, quit the operating system and reboot back into our usual interface.

V. CRIMES IN DARK WEB

In the criminal world, the most of the criminal activities are done in the Dark Web. So, the 'Dark Web' is called the center of the criminal attacks.

In 2013, the Federal Bureau of Investigation (FBI) arrested Ross Ulbrich for operating online illicit drugs market place called 'Silk Road'.

The following are some renowned crimes on dark web –

1) *Frauds Carding:* A user's personal information and card credentials selling are called as a fraud. It is the most popular sort of crime and also well-known scam on the dark web. Debit and credit cards are accessible for buying on darknet market place.
2) *Drugs Trafficking:* The dark web is an illegal marketplace for selling harmful drugs. They trade drugs in exchange for cryptocurrencies. A Canadian was started the dark web's largest darknet market which was shut down by the U.S police. Now the world largest drug market place is Alpha Bay in dark web.
3) *Onion cloning:* Cloning onions is a proxy method. Where the scammer duplicates the original site of page and changes the send the user to their scammed sites. This is the scam to make money from the users.
4) *Human Trafficking:* The human trafficking is occurred in the location of 'Black Death' on the dark web. The British model Chloe Ayling is sufferer of human trafficking on dark web. Black death is a dark web group that operates through often changing URLs.
5) *Hitman Hiring:* A professional killer can be hire from the dark web platform. Some of the groups of the murder-for-hire include unfriendly solution, hitman network etc. The group unfriendly solution receives the payment only in bitcoins.
6) *Information Leakage:* For whistle-blowers, activists and law enforcement, TOR is the most powerful tools. There are many nameless or unknowledgeable supporting networks out there. Hackers are used the dark web to disclose critical information. In 2017, 1.4 billion personal information was expose in text form on dark web and was easily obtainable on the internet employees are paid to expose company secrets by dark web hubs.

VI. RED ROOM & SILK ROAD

1) *Red Room:* A red room are supposed to be a myth, an urban legend. 'Red Room' sites, the story goes, are dark web sites where users pay thousands to watch rapes and murders live. This is a hidden website or service on the "dark web" where user can view or participate in interactive torture or murder. The dark web is a hidden collection of internet sites accessible only by a specialized web browser. It is used to keep internet activity anonymous and private, which can be helpful in both legal and illegal applications. Although some use it to evade government censorship, it is also known to be used for highly illegal activities. Accessing the dark web requires using an anonymous browser called Tor [9].
2) Silk Road: The Silk Road was a network of ancient trade routes. The vast trade networks of the Silk Road carried more than just merchandise and valuables. In fact, the constant movement and mixing of populations brought about a massive transmission of knowledge, ideas, culture and beliefs, which had a profound impact on the history and civilization of the Eurasian peoples. It is called the Silk Route because of the extensive silk trade during that period. This precious fabric originated in China, which initially had a monopoly on silk production until the secret of its creation spread. Apart from silk, the route facilitated trade in other textiles, spices, grains, fruits and vegetables, animal skins, wood and metal work, precious stones and other valuables [10][11].

Some Interesting Facts About Dark Web

- The dark web is a huge marketplace for criminals and earns at least $500,000 per day [12].
- Users mostly use bitcoins because they are virtually untraceable.
- It contains nearly 550 billion personal documents.
- More than 30,000 websites are hacked every day.
- There are more than 4.5 billion web pages on the "standard" Internet.

VII. CONCLUSION

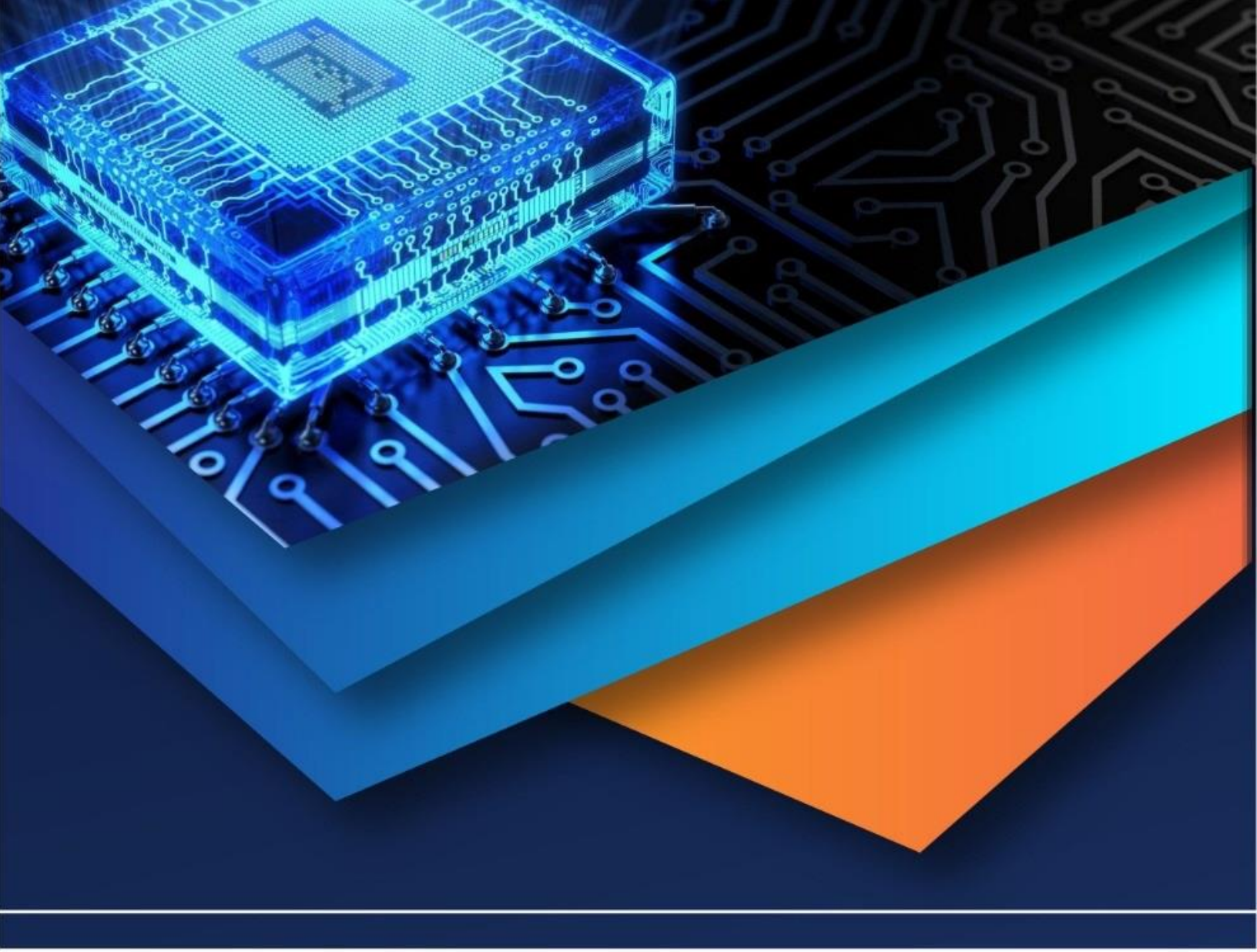
The dark web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address. While it's most famously been used for black market drug sales and even child pornography, the dark web also enables anonymous whistleblowing and protects users from surveillance and censorship.

In order to protect people's privacy and security, it is necessary to take action and address the issue of the encrypted nature of the dark web. The anonymity provided by complex algorithms which protect users' identities and deletes traces of them being on websites let to the most of the illegal and malicious activities to be performed on the dark web. The sheer difficulty of the dark web regulation let to the establishment of weapons and drugs marketplaces, and whole networks of websites used by terrorists for communication and propaganda.

There is a fine line between anonymity for the sake of privacy and anonymity as a cover for illegal activities. The encrypted nature of the dark web is a major challenge for the governments, and establishing new measures for tracking and preventing illegal and malicious activities on the dark web should be any countries' priority.

REFERENCES

[1] Jamie, B. (2014). The Dark Net.
[2] Lightfoot, S., & Pospisil, F. (2017). Surveillance and privacy on the deep Web. ResearchGate, Berlin, Germany, Tech. Rep.
[3] Senker, C. (2016). Cybercrime & the Dark Net: Revealing the hidden underworld of the internet. Arcturus Publishing.
[4] Henderson, L. (2022). Tor and the dark art of anonymity (Vol. 1). Lance Henderson.
[5] Diodati, J., & Winterdyk, J. (2021). Dark Web: The Digital World of Fraud and Rouge Activities. In Handbook of Research on Theory and Practice of Financial Crimes (pp. 477-505). IGI Global.
[6] Gehl, R. W. (2018). Weaving the dark web: legitimacy on freenet, Tor, and I2P. MIT Press.
[7] Ozkaya, E., & Islam, R. (2019). Inside the dark web. Crc Press.
[8] Inside the Dark Web – Erdal Ozkaya, 2019
[9] Beckstrom, M., & Lund, B. (2019). Casting light on the Dark Web: A guide for safe exploration. Rowman & Littlefield.
[10] Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. The British Journal of Criminology, 60(3), 559-578.
[11] Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.
[12] Davenport, D. (2002). Anonymity on the Internet: why the price may be too high. Communications of the ACM, 45(4), 33-35.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY