Dark Web Access, Hidden Services and Security Challenges

By **Mohammed Bilal**

***Abstract*-The dark web is a part of the world wide web however it is only accessible with the use of specific software and configuration. This paper will aim to provide information on how to access the dark web as well as the services being offered, and the security challenges present within the dark web. The dark web has always been in constant debate over whether users should be allowed complete anonymity due to the awful services which are present within the dark web. There are still however a few positives such as the access to information and complete anonymity however these positives are heavily outweighed by the negatives available upon the dark web.**

Keywords: Dark web, Tor, the onion router, anonymity, deep web, cyber.

I. INTRODUCTION

Advancements in technology over the years has resulted in decades of different cyber-attacks, many organizations over the years have huge concerns over web security due to the demand of people utilizing the web to complete their needs. In the 1990's, the US department of defense created an encrypted network which was also anonymized to protect confidentiality, this allowed them to communicate without any peering eyes or leaks [1].

The dark web refers to websites that are not indexed by search engines such as Google, these websites are accessed using Tor also known as The Onion Router. Although there are many illegitimate reasons to access the dark web there are also some heavily positive reasons people utilize the dark web. Those who fear from political prosecution from their governments use the dark web to communicate and access hidden information. Tor can prevent someone watching your connection and preventing them from knowing what websites you have accessed and visited.

The Tor network disguises the user's identity by encrypting all the user's traffic and moving it with the use of Tors network relays this aids in concealing the user's data and locational data. The use of the dark web often means that the user is attempting to engage in activity which wouldn't be possible in the public eye. The dark web is a subset of the deep web. The dark web has often been connected to criminal activity due to the services and goods offered, illicit goods and heinous crimes are just some of the nefarious services offered on the dark web [3]. However, many people utilize the dark web for legitimate reasons such as political dissidence and private communication. This paper will provide information on how to access the dark web and overcome many of the security challenges that reside within to maintain complete anonymity. This paper will also discuss the benefits and disadvantages the dark web can offer to its users.

II. DISCUSSION

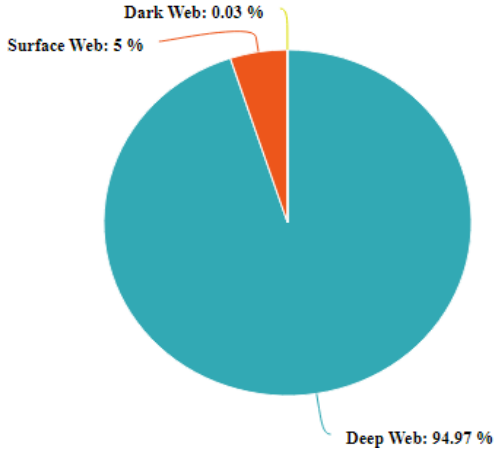
There are three types of web, surface web, deep web and lastly the dark web. The surface web is well known to every person and used every single day, the deep web consists of parts of the internet which are hidden from the eye of the public. An example of the deep web can be your email, it is not accessible by the public but can be used by the owner. The dark web consists of areas of the internet which are hidden intentionally and securely to keep them from the view of the public, the dark web is an area where anonymity is of utmost importance as stolen data, illicit activity and illegal media can be found and purchased here [3].

The surface web has always been a part of the World Wide Web since the first browser was invented. The surface web is equivalent to just 5% of the internet whereas the deep web is equal to 96% of the internet. The deep web is every set of data that is not indexed or even controlled within in the public surface web thus meaning it's also not publicly accessible [4]. Below is a table discussing the surface web, deep web and dark web.

Surface Web	**Deep Web**	**Dark Web**
Readily available for the general public to use daily without any added software.	Can be accessed by a direct URL or IP address may require a password or other security.	Special software such as Tor required to gain access.
Content can be found through any search engine such as Google or Firefox...	Content cannot be found through any search engine as not indexed.	Content is hidden intentionally from the public eye.
Contents of the surface web are legal and available.	Contents of the deep web are mostly a mix of both legal and illegal.	Contents of the dark web are more than often considered illegal.

The above table shows the dark web and the deep web have more in common than the surface web. The dark web is a subset of the deep web to be exact a small fraction of 0.03%. The number of dark websites equals up to the thousands which is not a lot however they are mostly encrypted thus the criminal activity as the users are kept anonymous and safe. An example of this is silk road, an online marketplace that resided on the dark web and was operated as a Tor hidden web service allowing users to browse anonymously without traffic monitoring [12]. The deep web however also contains sites such as password protected email accounts and paid subscription services such as Netflix or Amazon Prime as these are sites that can only be accessed by an online form. The deep web contains numerous legal and illegal content [5]. The deep web is sighted to be almost 500 times larger than

the surface web, most people do not realise they use the deep web almost daily to carry out the fulfilment of their needs. The main difference between the deep web and the dark web is to access the dark web Tor is required, Tor browsers can create encrypted entry points and pathways for the user keeping the websites and path they used to reach there encrypted, this way identities of the darknet users are kept securely hidden and are unable to be tracked or followed due to the encryption security provided by Tor [14,15]. The size of each of these three webs is shown in the below figure.



Pie chart portrays the size difference between the three webs.

III. How do users gain access to the dark web

Access to the dark web is a task that sounds simple but if done wrong can lead to several issues which may severely affect the user's life. Most users utilise Tor to gain access to the dark web and visit the websites as they are all onion websites. Within the deep web the dark web is also evolving making it much easier to navigate however there are still some precautions users take [10].

However operating systems such as Windows can lead the user to more problems as the OS constantly syncs data, browser history, app settings and voice assistants such as Cortana collect data such as keystrokes search results and audio messages. These reasons make the operating systems such as Windows 10 not the best to access the dark web. Regarding your reason for accessing the dark web, the users main concern should always be anonymity to ensure they are safe and secure [17]. Many people make use of VPNs to help provide an extra layer of security in case they do endure a mishap as a VPN is able to encrypt the user's internet traffic it is always a good idea to be safe than sorry.

IV. Is using tor illegal?

The use of the Tor browser is completely legal unless you reside in a country like China that actively blocks access to the Tor network. The Tor browser has the capability to facilitate or commit crimes [6]. The privacy offered by a browser like Tor is extremely important in the digital age today, as many corporations and hackers partake in unauthorised surveillance of online activity [2]. However, Tor can be used to partake in illegal actions which could incriminate the user despite Tor's legality.

V. Am i safe to be using tor on the dark web?

The Tor browser is very secure as the dark web consists of over 30,000 Tor network websites, if the Tor browser is being downloaded directly from the Tor website and not any 3rd party website [9]. As Tor encrypts your entry points and exit points you are safe from any prying eyes, the encryption applied by the Tor browser protects the user when surfing through the dark web.

VI. Is using the dark web illegal?

In most parts of the world accessing the dark web is completely legal and will not result in any type of prosecution. If you utilise the software and gain access to the dark web if you do not partake in any actions which violate the law, it is 100% legal. Carrying out illegal acts within the dark web or partaking in an activity that is illegal can result in the user being caught and prosecuted. Many people do access the dark web daily as it provides anonymity and helps keep their identity safe, others also access the dark web daily as it allows them to express their voice without any political dissent [19]. However, there are many black hat hackers present within the dark web who partake in malicious acts which can affect many people around the world these acts are performed for their own enjoyment and malice.

VII. Are there any benefits to using the dark web?

Although the dark web is assumed to all be criminal activity, there are several advantages for the users such as user anonymity, privacy/free speech and virtually untraceable sites and services.

User anonymity is one of the greatest benefits to using the dark web as the user's data is all encrypted this allows the user to access whatever they wish without having their network traffic being monitored.

Privacy and free speech another benefit of the dark web, which is like user anonymity, in today's digital age many people cannot express themselves freely on social media due to political dissident and employers may not agree with their views which can result in them losing their livelihood however on the dark web thanks to the level of encryption making it practically untraceable, they are able to express their views whether that be political or something else [20].
Virtually untraceable services and sites allow users to access information which will not be available in the public eye without their identity being exposed. Many services/sites on the dark web are heavily encrypted which is beneficial to the user as they will not have to worry about any network traffic monitoring while completing their transaction.

VIII. Disadvantages of using the dark web

Malware, scams, illegal activity are just some of the disadvantages of utilising the dark web.
The dark web is very well known for malicious activity such as the sale of narcotics. The main disadvantage of the dark web is certain individuals abuse the power and anonymity of the dark web, as the dark web does promise privacy to its users it has also been used to violate the privacy of others by

sharing people's private photos, medical records and financial information.

Another disadvantage of using the dark web is hackers can implement malware to users if the user is not correctly protected and there is an array of scams present on the dark web which if the user does fall trap to, they could end up giving away personal information without intending to.

IX. Hidden services and activities on the dark web

The dark web is known for facilitating a array of crimes such as the sale of drugs, guns, exotic animals and stolen goods. Among these there are also several dark services such as thieves and assassins for hire. Illicit marketplaces on the dark web provide criminals with an array of illicit commodities [9]. There are many illegal items available within the dark web many of which are hidden unless the user is invited or trusted by another user. The most publicised website of the dark web is silk road marketplace for many illicit goods [7]. These hidden services available on the dark web have an IP address hidden from the outside world which allow for the website to be untraceable. The URL of these websites comprises of 16 characters that are very difficult to comprehend and find without knowing of them.

X. Threats on the dark web

There is an abundance of threats within the dark web, some of these are viruses, scams, fraud, malware, illegal activity and government-controlled Tor websites.

Malware such as botnets, phishing malware and key loggers are all over the dark web and attack unsuspecting users just as they do on the surface web, if your connection can be exploited this can lead to many issues which may affect the user's life outside of a screen. Key loggers can record your keystrokes and searches thus showing the attacker the path you have navigated and what website you may attend.

Ransomware a form of malware designed to encrypt a user's files on a device which in turn makes the device unusable and unreliable, in return for the user's files cyber criminals demand a ransom for the data to be released. If your connection on the dark web is exploited your device may be held with ransomware the worst part about this is there's no guarantee the attacker will release your data even after payment [21]. The money is often paid in cryptocurrency such as bitcoin thus making it even harder to trace the perpetrator.

Fraud is very common on the dark web as criminals try to defraud new and unsuspecting users of the dark web, by sending them to a certain webpage in the dark web which may ask for private details which hackers will save and will cause problems for the user. Fraud on the dark web is often hidden very well and does not look suspecting at all. Illegal dark web forums sell stolen credit credentials and use stolen information and phishing malware to appear more authentic.

Another threat of the dark web is you may not realise and stumble upon illegal activity without intending to, the website may look as if it is something simple and not at all many illegal websites upon the dark web utilise this technique to ensure more privacy for themselves. Illegal activity on the dark web can be of many things such as assassination and its marketing, drug transactions and extremist views [8].

Government monitoring is another threat of the dark web. As many Tor websites are being overtaken by authorities all around the world there is a significant risk of becoming a target for the government even if you accidentally access a government-controlled Tor website on the dark web. Illegal drug marketplace such as the infamous silk road has been used for surveillance by the authorities. Utilising custom software to analyse activity has allowed the authorities to identify users, this may result in you being watched by security organisations even if you haven't done anything wrong.

XI. Steps to stay safe when accessing the dark web

There are multiple steps to safely accessing the dark web and ensuring an encrypted channel to help protect your anonymity. Follow the steps below to help ensure your anonymity and safety when surfing the dark web.

Disable Java/ActiveX in the available network settings. These frameworks are well known for getting exploited by malevolent parties. As the dark webs network is full of unknown threats its best to avoid all risks.

Utilise a non-admin local account, this is necessary as most main accounts on computers will have full admin permissions enabled. Malware utilises this to implement its functions, with a non admin local account without the admin permissions the malware can be slowed down and halted even. Avoiding document downloading will also ensure a much safer practice as most documents on the dark web have malware embedded.

Restrict access to your Tor enabled device as this will protect your children/family and unwanted eyes from accessing the dark web and seeing something they should not see. Trusting your intuition is also key as this will help the user to avoid being scammed, staying safe and secure is a necessity as many people on the dark web are not who they claim to be, if something does not feel right remove yourself from that situation this could be a website or even a service that seems odd.

Many online security services now offer identity protection for the user’s safety be sure to make use and take advantage of these tools to help ensure your identity is safe from any attempts of identity theft or fraud as this is quite common on the dark web where users identities have been compromised thus has affected their lives tremendously [22]. Remove your online persona from real life this includes email addresses, usernames, real name and even passwords as this will help protect the users identity and keep them safe. When making a purchase on the dark web utilise pre-paid debit cards and throwaway accounts as this will help secure your anonymity and disguise your real-life identity from your online persona.

XII. Conclusion

In conclusion, the dark web which is a subset of the deep web and has positives as well as negatives. The dark web does have an immense amount of criminal activity occurring daily from the selling of drugs to the purchase of stolen identities. However, the dark web also serves many people in a positive light too due to political dissidence and whistleblowing, journalists can share their views and thoughts without any

repercussion thanks to the encryption levels deployed by Tor. The dark web allows people to express their views without receiving any real-life backlash. The dark web is a great way to preserve your right to anonymity and freedom however it also has severe criminal attributes. The dark web can only be accessed using specialised browsers such as Tor. To summarise the dark web is a place of information and anonymity with its own benefits and downfalls.

REFERENCES

[1] Kaur, S. and Randhawa, S., 2020. Dark Web: A Web of Crimes. Patiala, India: Computer Science and Engineering Department, Thapar Institute of Engineering and Technology.

[2] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[3] Huang, H. and Bashir, M., 2016. The Onion Router: Understanding a Privacy Enhancing Technology Community. Illinois: University of Illinois, pp.6-8.

[4] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[5] Milosevska, T., 2020. DARK WEB – NEW TRANSNATIONAL SECURITY THREAT. France: FACULTÉ DE PHILOSOPHIE SKOPJE, pp.1-3.

[6] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 77-82, 2016.

[7] Gan, R., 2019. Dark and Deep Webs-Liberty or Abuse. Israel: Lev Topor, Bar Ilan University, pp.2-4.

[8] Mwila, K., 2018. The Deep Web. Zambia: University of Zambia, pp.3-4.

[9] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[10] Shavers, B. and Bair, J., 2016. The Tor Browser. p.1-2.

[11] Bradbury, D., 2014. Unveiling the dark web. p.2-4.

[12] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[13] NAZAH, S., HUDA, S., ABAWAJY, J. and HASSAN, M., 2020. Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. Riyadh, Saudi Arabia: King Saud University, pp.2-3.

[14] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.

[15] Madison, K., 2020. Tor And the Deep Web 2020: A Beginner's Guide to Staying Anonymous, Dark Net Journey on How to Be Anonymous Online. pp.5-9.

[16] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[17] Finklea, K., 2017. Dark Web. Congressional Research Service, pp.3-4.

[18] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[19] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.

[20] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.

[21] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[22] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.