A Mysterious and Darkside of The Darknet: A Qualitative Study

Afsana Anjum[i]; Dr. Chamandeep Kaur[ii] ; Sunanda Kondapalli[iii]; Mohammed Ashafaq Hussain[iv]; Ahmed Unissa Begum[v]; Samar Mansoor Hassen[vi]; Dr. Mawahib Sharafeldin Adam Boush[vii]; Atheer Omar S Benjeed[viii]; Dr. Mohammed Hassan Osman Abdalraheem[ix]

Received November 10, 2021; Accepted December 20, 2021
ISSN: 1735-188X

Abstract

Nowadays, the darknet or dark web has become one of the most booming topics in context with cyber security. [6]Several research studies and current reports conclude that how the anonymous nature of the darknet provides a platform for illegal activities and cybercrime. The dark web is a hidden online market for everything, including but not limited to human trafficking, drugs, illegal weapons, forged documents, hire services for murder, narcotics, indecent pornography, etc. Because of these reasons, it is difficult for digital forensic professionals to trace the origin of traffic, location, and ownership of any computer or person on the Darknet. This paper reveals the mysterious and invisible facts of the darknet in various ways.

Keywords

Dark web, TOR, Cybercrime, Privacy, deep web, cybersecurity, hacking, blackhat, security, darknet.

Introduction

Many of us are aware that the internet provides a platform for an information system known as the World Wide Web, where we can access and share any kind of information and this information is exchanged hugely by the community globally. But this community is unaware of the existence of an invisible or hidden layer of the internet that provides anonymity and a platform mostly used for illegal businesses and cybercrimes, known as darknet or deep web. The internet which we use for surfing and exchanging information is only 5% of the whole internet rest of the large part of the internet is invisible is called the deep web. The deep web is also called the invisible web, for some technical reasons its contents are not indexed.

An increasing number of cybercrimes and criminals are using the dark web-the encrypted part of the internet that cannot be tracked, to shop for software that helps them remain anonymous while carrying out their crimes. The dark web is a part of the deep web, the non-indexed part of the worldwide web that cannot be accessed by standard search engines such as Google and requires encrypted networks such as the Tor browser. This study illuminates information on the various layers of the Internet, with a particular focus on the Dark Web.

The Dark Web-Dictionary

Lots of people active on the dark web use abbreviations that are unclear to newcomers. That's why here I have mentioned the meaning of some commonly used abbreviations:

2FA

Two-factor authentication. [25] It is a simple way to secure your account. Instead of relying on a single password system, it is better to adopt this method to gain access to your account by using another device. Usually, this is done with a smartphone.

Alpha bay

[25] After the shutdown of the Silk Road website this became the big marketplace for the most buyers.

Blockchain

[25] This is the prominent technology of Bitcoin. It can be operated in 3 modes i.e., public, private, and hybrid mode on which crucial data can be stored and the transaction can be done safely and securely.

BTC

[25] This is the acronym given to Bitcoins. It is popularly known by cryptocurrency and widely used for anonymous transactions on the darknet.

Clearnet

[25] Simply put, the Clearnet is everything you can find on the internet via a search engine such as Google. These are all the publicly available websites, do not require any kind of registration or log-in credentials. However, this does not mean that websites that require a log-in are necessarily not part of the Clearnet.

LEA/LE

[25] Short for 'Law Enforcement Agencies/Law Enforcement. This is an acronym for Tor network users who wish to evade the scrutiny of law enforcement. These actors are present and active on dark markets, and they will try to frame you.

OS (Live or Host)

[25] Short for Operating System. Cybercriminals are using such OS like Windows, Mac, Linux and VirtualBox software to operate illegal activities on the darknet.

Red Rooms

[25] Red Rooms are a common myth of the Dark Web. Many people claim that certain types of websites exist where several people pay a fee, gain access to a live stream where there is a torturer and a victim. The Paid visitors of the stream would then be able to order the torturer into acting out any depraved desires the streamers might have. Thankfully, to this day, no actual report of a verified Red Room has ever come in. As far as we know, red rooms are full of fantasies rather than realities.

Silk Road

[25] This was the original 'success story of the dark web. A young man set up a completely free-market economy for people to compete in. It was shut down in 2013 and was mostly known for being a marketplace for drugs and weapons.

Tails

[25] Tails stands for: "The Amnesiac Incognito Live System." This is a live version of Linux that helps you install the OS on any device.

VPN

[16] This is short for a virtual private network. If a user uses VPN for illegal activities on the darknet than it is difficult for the Law Enforcement or cyber forensic officials to trace the cyber criminals on the darknet.

How Tor Browser works

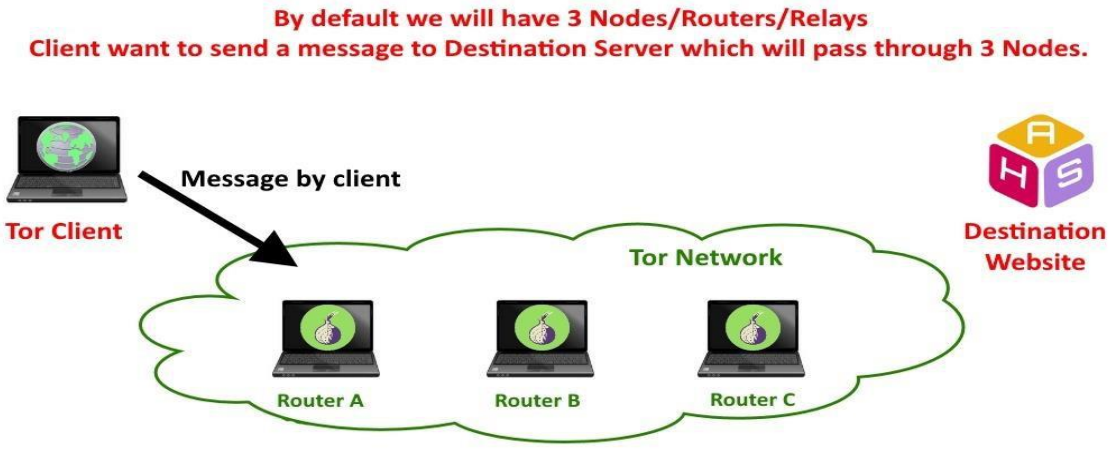
The onion Router is the abbreviation for TOR, is an open-source private network that allows the users to browse on the internet anonymously. The tor was initially developed and solely used by the U.S Navy to protect sensitive government communications before the network was made publicly available. The rapid improvement in the technology and innovation of digital products has been changed and has given way to frequent data breaches and cyber thefts in response consumers are increasingly opting for products that offer data privacy and cyber security.

Tor is an underground anonymous network that was implemented to hide the user's identities. The tor network is one example of the many emerging technologies that attempt to fill a data privacy void in a digital space plagued by cyber security concerns. The tor network intercepts the traffic from your browsers and bounces a user's request of a random number of the user requests final destination. These random users are volunteer devices which are called nodes or relays.

[27] The tor network disguises your identity by encrypting the traffic and moving it across different tower relays within the network, the tor network uses an onion routing technique for transmitting data hence the original name of the onion router to operate within the tor network a user has to install the tor browser. Any address or information requested using the browser is transmitted through the tor network, it has its own feature set. The data passing through the tor network must follow a unique protocol known as the onion routing protocol.

In our normal network usage, the data is transmitted directly the sender has data packets to transmit which is done directly over a line of communication with either a receiving server of the same kind. However, since the data can easily be captured while being transmitted the security of this exchange is not very reliable. Moreover, it becomes very easy to trace the origin of such requests on many occasions' websites with questionable and controversial content are blocked from the ISP. This is possible since the ISP can detect and spy on user information passing through the network. Apart, from ISPs, there is a steady chance of your private information being intercepted by hackers unfortunately easy detection of the sources and contents of a web request makes the entire network extremely vulnerable for the people who seek anonymity over the internet. However, the onion routing protocol things take a longer route. We have a sender with the tor browser installed on the client system.

The network sends the information to IP address of node one which encrypts the information and passes it on IP address of node 2 which performs another encryption and passes it on Ip address of node 3. This is the last address which is also known as the exit relay node. This last node decrypts the encrypted data and finally relays the request to the final destination which can be another device or a server end. This final address thinks the request came from the exit node and grants access to it encryption process across multiple computers repeats itself from the exit node to the original user. The tor obfuscates user IP addresses from unwanted surveillance by keeping the users request untraceable with multiple servers touching the data it makes the tracking very difficult for both ISPs and malicious attackers.



The above figure shows how the Tor works in a simplified way. It clearly shows the data that the Tor user will send will pass through these three Routers before going to the Destination.

Illegal Activities And Cybercrime

Many types of crime can be done online with secrete transactions, whether it involves drugs, money or even human beings can be done by using the dark web. That's why it is called the darkest corner of the internet "A platform for illegal business and cybercrime". Following are some hilarious examples of darknet crimes:

1. Contract killings
2. Extortion
3. Illegal drug sale
4. Illegal weapon sale
5. Sex trafficking
6. Recruitment and planning terror attacks
7. Child pornography and many more…

Several investigators and findings reported a same kind of crime happened on the darknet. This investigation led to the activity taking place on the dark web marketplaces and found many black markets good available on the Silk Road website. There are various illegal drugs like Ecstasy, LSD, heroin, and steroids are available on the darknet marketplace. Also, illegal weapons and books on how to construct bombs, counterfeit identification, and merchandise available on the darknet at very cheaper rates.

[38] Illegal drugs are one of the most dangerous goods available on the darknet marketplace. The reason behind this, the criminals or smugglers who buy and sell those illegal drugs online do not need to work hard to find customers. Drug consumers easily get trapped and

buy all the illegal drugs online on the darknet. But they are unknowingly keeping their life at risk by ordering and consuming these illegal and dangerous drugs anonymously.

Silk Road was the most dangerous, modern, and first online anonymous black-market place on the darknet. [6] Ross Ulbricht is the creator and founder of the Silk Road website. It was operated by using a hidden layer of the internet called dark web by using TOR browser, for providing hidden goods and services to the customers online, so that online users were able to buy any available goods anonymously and securely without being monitored. The website of Silk Road was launched in February 2011, within a few years Silk Road has provided goods and services to more than 1,00,000 buyers online. It has been estimated that Silk Road has generated revenue of approximately 1.2 billion dollars. Payments in this market are, expectedly, made in crypto-currency such as Bitcoin, which has no central issuing authority and permits anonymous transactions. In 2013 media reports had estimated that 12 million Bitcoins were in circulation; at present, one Bitcoin is worth $300-335. In, October 2013, the website was shut down and Ross Ulbricht was get arrested by the Federal Bureau of Investigation (FBI). They investigate and found that people from around the world are buying and selling illicit drugs, weapons, and poisons and provide services for hacking and murders. On February 4, 2015, Ross Ulbricht was sentenced to two life sentences and 40 years without the possibility of parole.

Nowadays children are increasingly becoming victimized in human trafficking, as they are forced to be labor and the commercial sex trade. Despite making the best efforts of the government to stop these activities on the dark web, the hidden nature of the darknet makes it very difficult to trace the people on the darknet. Many criminal organizations shifted the business of human trafficking on the darknet because it is easy to operate, cheaper, and exploits more children there. Because of these circumstances, undoubtedly, the darknet has become the safest place and anonymous for human trafficking and pornography.

One of the most recent and notorious human trafficking groups comes into the picture named "The Black Death Group" of Eastern Europe, which operates all its business on the darknet. The business involved not just adult and child trafficking with selling sex slaves to Saudi Arabia, but it also hosted auctions of virgin young girls of 15 years of age, advertising them by their looks including age, hair color, and measurements. The starting price in this auction can be as high as $760000, with the disclaimer that "They do not sell girls who are ill, pregnant, have AIDs or are young mothers.

The most recent case has been reported against the abduction of the victims by the "Black Death Group". They have been accused of kidnapping a 21 years old British model, who claimed that she had been drugged badly and stuffed in a suitcase. She has been harassed, tortured, and abused for 6 days, and also, she has been warned that she would be auctioned to the buyers on the darknet and then fed to the tigers if she refused. She was later told that she would be auctioned as a sex slave for $354780.

[37] Darknet is also the safest and perfect place for child trafficking and pornography. Several websites on the darknet allow number of users to share strategies on targeting, seducing, and engaging in sexual attacks on teenagers in various ways. One of the famous owners of child play from Canada named Benjamin Faulkner runs a child pornography website on the darknet and that is at its peak with over 1 million profiles. The website showcases short videos of over 100 producers of porn videos who raped and brutalized children and women. After running the website for about 6 months, Benjamin Faulkner gets captured along with his associate Patrick Falte by the United States Department of Homeland security, in October 2016. [36] Patrick was arrested with all his devices which contains a collection of child porn images and videos. There are approximate 45000 images and 2500 videos of child porn. The website name "The Giftbox Exchange", another mysterious child pornography website on the darknet get shut down by the officials in November 2016 and they both are sentenced to life imprisonment.

Conclusions

The darknet is the perfect platform for illegal business and criminal activity, as it is anonymous and not visible by using many standard search engines, it is a great platform for cybercriminals and traditional criminals as well. A darknet is also a powerful tool and black-market place where you can find several goods and services like pirated software, illegal drugs, weapons, and many programmed viruses for hacking. Along with those tools, it is a perfect place to buy and sell the data that is stolen from the various databases by data breaches that are so common in the modern world.

Despite the many efforts of the government, the hidden nature of the deep web makes it very difficult to trace people. [35] Though law enforcement and cyber forensic agencies have been continuously working to stop these activities, there are huge numbers of people who operate the darknet, which makes it difficult for the agencies to investigate and find them.

As a responsible citizen and a wise human being, it is our responsibility to show empathy toward one another. If somebody is being exploited today, then it is possible tomorrow that might happen it to us also. We must raise our voice against this and join to help each other, educate each other, and take steps to end human trafficking and pornography.

Bibliography

[1] M. Chertoff, “A public policy perspective of the Dark Web,” J. Cyber Policy, vol. 2, 2017, doi: 10.1080/23738871.2017.1298643.

[2] Sydney Butler, “The Role of PGP Encryption on the Dark Web,” Feb. 2019.

[3] A. S. Beshiri and A. Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," J. Comput. Commun., vol. 07, no. 03, pp. 30–43, 2019, doi: 10.4236/jcc.2019.73004.

[4] Z. Mohamud Omar and J. Ibrahim, "An Overview of Darknet, Rise and Challenges and Its Assumptions," Int. J. Comput. Sci. Inf. Technol. Res., vol. 8, no. July, pp. 110–116, 2020, [Online]. Available: www.researchpublish.com.

[5] M. & A. Gupta, "The Dark Web Phenomenon: A Review and Research Agenda," p. 12, 2019.

[6] M. Mirea, V. Wang, and J. Jung, "The not so dark side of the darknet: a qualitative study," Secur. J., vol. 32, no. 2, pp. 102–118, 2019, doi: 10.1057/s41284-018-0150-5.

[7] M. Trelstad, "Introduction to death," Dialog, vol. 57, no. 4, pp. 229–234, 2018, doi: 10.1111/dial.12424.

[8] S. Kaur and S. Randhawa, "Dark Web: A Web of Crimes," Wirel. Pers. Commun., vol. 112, no. 4, pp. 2131–2158, 2020, doi: 10.1007/s11277-020-07143-2.

[9] A. Parkar, S. Sharma, and S. Yadav, "INTRODUCTION TO DEEP WEB," Int. Res. J. Eng. Technol., 2017, [Online]. Available: https://danielmiessler.com/study/internet-deep-.

[10] Rajesh E, "Issue 4 www.jetir.org (ISSN-2349-5162)," 2019. [Online]. Available: www.jetir.org.

[11] A. Gupta, S. B. Maynard, and A. Ahmad, "The Dark Web Phenomenon: A Review and Research Agenda."

[12] A. S. Beshiri and A. Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," J. Comput. Commun., vol. 07, no. 03, pp. 30–43, 2019, doi: 10.4236/jcc.2019.73004.

[13] J. R. and R. A. L. and W. M. A. Liggett Robertaand Lee, "The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets," in The Palgrave Handbook of International Cybercrime and Cyberdeviance, A. M. Holt Thomas J.and Bossler, Ed. Cham: Springer International Publishing, 2020, pp. 91–116.

[14] S. Kaur and S. Randhawa, "Dark Web: A Web of Crimes," Wirel. Pers. Commun., vol. 112, no. 4, pp. 2131–2158, Jun. 2020, doi: 10.1007/s11277-020-07143-2.

[15] Z. Mohamud Omar and J. Ibrahim, "An Overview of Darknet, Rise and Challenges and Its Assumptions," Artic. Int. J. Comput. Sci. Inf. Technol., vol. 8, pp. 110–116, 2020, [Online]. Available: www.researchpublish.com.

[16] M. Mirea, V. Wang, and J. Jung, "The not so dark side of the darknet: a qualitative study," Secur. J., vol. 32, no. 2, pp. 102–118, Jun. 2019, doi: 10.1057/s41284-018-0150-5.

[17] S. Handa and J. Lenz, "An Introduction to the Dark Web," 2021. [Online]. Available:

www.blakes.com,.

[18] M. Chertoff, "A public policy perspective of the Dark Web," J. Cyber Policy, vol. 2, no. 1, pp. 26–38, Jan. 2017, doi: 10.1080/23738871.2017.1298643.

[19] S. Kaur and S. Randhawa, "Dark Web: A Web of Crimes," Wirel. Pers. Commun., vol. 112, no. 4, pp. 2131–2158, 2020, doi: 10.1007/s11277-020-07143-2.

[20] K. Kruithof, J. Aldridge, D. D. Htu, M. Sim, E. Dujso, and S. Hoorens, Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. Santa Monica, CA: RAND Corporation, 2016.

[21] Phoebe Moloney, "Dark net drug marketplaces begin to emulate organised street crime," Jan. 2016.

[22] Etay Maor, "The Darknet Isn't Just for Dark Deals," Feb. 2015.

[23] T. McLennan, "An Introduction to the Dark Web - HUB Blog," 2020, [Online]. Available: https://www.hub.ca/newsletter-content/an-introduction-to-the-dark-web.

[24] Y. Expressway, G. Noida, and U. Pradesh, "A Research Paper on Dark Web," vol. 6, no. 4, pp. 322–327, 2019.

[25] Ms. Sonali Sagar Kharade, "A Study of Darknet: A Platform for Illegal Business and Cybercrime ," IDEES –International Multidiscip. Res. J. (Peer Rev., vol. 6, no. 2, pp.1001–1010, Jun. 2020.

[26] G. P. Paoli, J. Aldridge, N. Ryan, and R. Warnes, "Chapter title A Behind the curtain The illicit trade of firearms, explosives and ammunition on the dark web," 2017. [Online]. Available: www.rand.org/t/RR2091.

[27] B. Evers et al., "Thirteen Years of Tor Attacks."

[28] J. Wright, "Darknet Usage in the Illegal Wildlife Trade," 2019, doi: 10.31235/osf.io/fgr9d.

[29] W. Lacson and B. Jones, "The 21st century Dark Net market: Lessons from the fall of silk road," Int. J. Cyber Criminol., vol. 10, 2016.

[30] M. C. Hout and T. Bingham, "'Silk Road', the virtual drug marketplace: A single case study of user experiences," Int. J. Drug Policy, vol. 24, 2013, doi: 10.1016/j.drugpo.2013.01.005.

[31] I. Naseem, A. K. Kashyap, and D. Mandloi, "Exploring anonymous depths of invisible web and the digi-underworld," Int. J. Comput. Appl., vol. NCC, 2016.

[32] E. Çalışkan, T. Minárik, and A.-. M. Osula, Technical and legal overview of the tor anonymity network. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

[33] M. Mirea, V. Wang, and J. Jung, "The not so dark side of the darknet: A qualitative study," Secur. J., vol. 32, 2018, doi: 10.1057/s41284-018-0150-5.

[34] M. Mirea, V. Wang, and J. Jung, "The not so dark side of the darknet: a qualitative study," Secur. J., vol. 32, 2019, doi: 10.1057/s41284-018-0150-5.

[35] R. GUPTA, "The Darknet: A Safe Haven for Human Trafficking," onebread,2021.https://onebread.org/blog/2021/3/15/the-darknet-a-safe-haven-for-human-trafficking.

[36] J. MURALI, "Human-trafficking on the dark-web," DECCAN CHRONICLE, 2019.

[37] J. Kanics, "Child Trafficking and Ireland," Stud. An Irish Q. Rev., vol. 97, no. 388, p. 16, 2008, [Online]. Available: https://www.jstor.org/stable/25660604.

[38] P. S. K. Hazel Kwon, J. Hunter Priniski, Soumajyoti Sarkar, Jana Shakarian, "Crisis and Collective Problem Solving in Dark Web," in Proceedings of the 8th International Conference on Social Media & Society,

[i] Lecturer, Computer Science Department, Jazan University, Saudi Arabia. Email: elex786@yahoo.com

[ii] Lecturer, Computer Science Department, Jazan University, Saudi Arabia. Email: kaur.chaman83@gmail.com

[iii] Lecturer, Computer Science Department, Jazan University, Saudi Arabia. Email: gva.sunanda@gmail.com

[iv] Lecturer, Computer Science Department, Jazan University, Saudi Arabia. Email: mahussain@jazanu.edu.sa

[v] Lecturer, Computer Science Department, Jazan University, Saudi Arabia. Email: asrakhan3@gmail.com

[vi] Lecturer, Computer Science Department, Jazan University, Saudi Arabia. Email: shassen@jazanu.edu.sa

[vii] Assistant Professor, Computer Science Department, Jazan University, Saudi Arabia. Email: mboush@jazanu.edu.sa

[viii] Teaching Assistant, Computer Science Department, Jazan University, Saudi Arabia. E: atheeer1992@gmail.com

[ix] Assistant Professor, Computer Science Department, Jazan University, Saudi Arabia. E: mohammedh@jazanu.edu.sa