The Darkweb

Article · February 2023

Shoumik Chandra
Lovely Professional University

The Darkweb

Shoumik Chandra
School of Computer Science & Engineering
Lovely Professional University
Phagwara, Punjab
e-mail:
chandrashoumik.1999@gmail.com

***Abstract*—The Darkweb, is a hidden part of the internet that is not indexed by search engines and can only be accessed using specialized software, such as Tor. The Darkweb is often associated with illegal activities, such as the sale of drugs, weapons, and stolen data. However, it is also used for legitimate purposes, such as anonymity and free speech. This paper provides an overview of the Darkweb, including its definition, background, types of content, and the anonymity and security provided by it. Additionally, the paper discusses the impact of the Darkweb on society, efforts to regulate and shut down the Darkweb, current state and future trends, as well as ethical and moral issues associated with it. The paper concludes by emphasizing the importance of considering the potential harms and benefits of the Darkweb when discussing its regulation and use.**

***Keywords*—tor; hidden service; dark web; attack and defense of anonymous; dark web crawler; dark web data mining; understanding dark jargons**

I. Introduction

The dark web is a part of the internet that is not indexed by search engines and can only be accessed using specialized software, such as the TOR network. The anonymity provided by the dark web has made it a popular destination for illegal activities, such as the sale of illegal drugs and weapons, and the posting of stolen personal information. However, the dark web also has legitimate uses, such as for political dissidents and journalists operating in oppressive regimes, and for individuals seeking to protect their privacy. This review paper will provide an overview of the different components that make up the dark web, discuss the various methods used to attack anonymity on the dark web and the measures that can be taken to defend against such attacks, explore the use of dark web crawlers for data collection and the ethical and legal considerations of dark web data mining and understanding the dark web jargons.

II. Component

The dark web is composed of several different components that work together to provide anonymity and access to hidden services. One of the most important components of the dark web is the TOR network.

TOR, short for The Onion Router, is a network of volunteer-run servers that allows users to browse the internet anonymously. The TOR network works by routing internet traffic through multiple layers of encryption, making it difficult to trace the origin of the traffic. The use of TOR provides a great deal of anonymity, but it also has some drawbacks. For example, the use of TOR can slow down internet speeds and make it more difficult to access some websites.

TOR is a free and open-source software that enables anonymous communication by routing internet traffic through a network of volunteer-operated servers, known as nodes. Each node in the TOR network only knows the location of the previous and next node in the path of the internet traffic, making it difficult to trace the origin or destination of the traffic (Dingledine, Mathew, & Syverson, 2004).

Another important component of the dark web is hidden services. These are websites that can only be accessed through the TOR network, and their location and operators are concealed. Hidden services are created using the TOR network's hidden service protocol, which allows for the creation of virtual private networks (VPNs) on top of the TOR network (Murdoch & Danezis, 2007).

III. Tor

TOR is a network of volunteer-run servers that allows users to browse the internet anonymously. The TOR network works by routing internet traffic through multiple layers of encryption, making it difficult to trace the origin of the traffic. The use of TOR provides a great deal of anonymity, but it also has some drawbacks. For example, the use of TOR can slow down internet speeds and make it more difficult to access some websites. Additionally, the anonymity provided by TOR is not foolproof, and there have been cases of users being de-anonymized through various methods such as traffic analysis and browser fingerprinting.

IV. Hidden Services

Hidden services are websites that can only be accessed through the TOR network and are not indexed by traditional search engines. These services are typically hosted on the dark web and provide a high level of anonymity for both the website owners and users. Examples of commonly used hidden services include drug marketplaces and whistleblower platforms.

One of the most well-known examples of a dark web hidden service is the Silk Road, which was a notorious online marketplace for illegal drugs. The Silk Road was eventually shut down by law enforcement, but similar marketplaces continue to exist on the dark web. Other examples of hidden services include platforms for anonymous communication and file sharing, such as the now-defunct platform known as Freedom Hosting.

The anonymity provided by the dark web has made it a popular destination for illegal activities, such as the sale of illegal drugs and weapons, and the posting of stolen personal information (Van der Meijden, & Van Eeten, 2018). The Federal Bureau of Investigation (FBI) estimates that the dark web is used for around 20% of all cybercrime (Cresci, 2015). The most popular marketplaces on the dark web are used to buy and sell illegal drugs, with the most popular being the now-defunct Silk Road (D'Angelo, 2016).

V. Legitimate Uses of the Dark Web

While the dark web is often associated with illegal activities, it also has legitimate uses. For example, political dissidents and journalists operating in oppressive regimes can use the dark web to communicate and share information without fear of censorship or surveillance (Kshetri, 2018). Additionally, individuals seeking to protect their privacy can use the dark web to communicate and share information without fear of being tracked or monitored.

VI. Dark Web

The dark web has a long and complex history, dating back to the early days of the internet. The first iteration of the dark web was a collection of underground bulletin board systems (BBS) that were only accessible via dial-up connections. As the internet evolved, so did the dark web. The development of TOR and other anonymity-providing technologies made it possible for individuals to access and operate hidden services on a larger scale.

VII. Methods of Attacking Anonymity

There are several methods that can be used to attack the anonymity provided by the dark web. One method is traffic analysis, which involves analyzing patterns in internet traffic to identify the source and destination of the traffic (Panchenko, & Zajcev, 2016). Another method is browser fingerprinting, which involves identifying a user by their browser's unique configuration, such as installed fonts and browser plugins (Eckersley, 2010). Law enforcement agencies and other organizations have also developed methods for identifying and tracking users on the dark web, such as by infiltrating dark web marketplaces and using malware to track users (Europol, 2017).

VIII.Methods of Defending Against Attacks

There are several measures that can be taken to defend against the methods of attacking anonymity on the dark web. One measure is using the TOR network's built-in security features, such as using the TOR browser and enabling the NoScript plugin (TOR Project, 2020). Another measure is using a VPN in conjunction with the TOR network to add an extra layer of encryption and protection (BestVPN, 2021). Additionally, using secure communication methods such as encrypted messaging apps can also help protect against attacks (WhatsApp, 2021; Signal, 2021). It is also important for users to be aware of the risks associated with using the dark web and to take steps to protect their identities.

IX. Dark Web Crawler

Dark web crawlers are specialized software programs that are used to automatically browse and collect data from hidden services on the dark web. These crawlers can be used for a variety of purposes, such as tracking illegal activities, identifying potential security threats, and conducting research.

However, the use of dark web crawlers raises several ethical and legal considerations. For example, the collection of data from hidden services without the consent of the operators or users may be considered a violation of privacy. Additionally, the use of dark web crawlers may also be illegal in certain jurisdictions.

X. Dark Web Data Mining

Dark web data mining is the process of collecting, analyzing, and interpreting data from the dark web. This can include data from hidden services, forums, and other sources. The goal of dark web data mining is to gain insights into the activities and behaviors of users on the dark web.

Dark web data mining can be used for a variety of purposes, such as identifying potential security threats, tracking illegal activities, and conducting research. However, it also raises several ethical and legal considerations. For example, the collection of data from the dark web without the consent of the users may be considered a violation of privacy. Additionally, the analysis and interpretation of dark web data may also be subject to legal limitations.

XI. Understanding Dark Web Jargons

The dark web is often associated with illegal activities and is therefore associated with a lot of jargon and terminology. To understand the dark web, it is important to familiarize oneself with the jargons used on the dark web. For example, the term "onion" is often used as a metaphor for the layers of encryption and protection provided by the TOR network (TOR Project, 2020). Additionally, the term "clearnet" is used to refer to the regular internet, as opposed to the dark web (Kshetri, 2018). Other terms include "red rooms", which are urban legends of hidden services on the dark web where live torture and murder are streamed, but there is no evidence that these exist (Whitty, & Buchanan, 2019). Understanding these terms is important for anyone interested in the dark web, whether for research or personal use.

Some examples of common dark web jargon include:

- Cryptocurrency: The dark web primarily uses cryptocurrency for transactions. Bitcoin is the most widely used cryptocurrency on the dark web.
- Escrow: A system of trust used to facilitate transactions on the dark web. Escrow is used to ensure that both parties involved in a transaction are satisfied before releasing payment.
- PGP: PGP stands for "Pretty Good Privacy" and is a widely used encryption method on the dark web. It is used to secure communications and transactions.

XII. Impact on society

The darkweb has had a significant impact on society, primarily because of the illegal activities that take place on it. The sale of illegal drugs on the darkweb has been linked to the opioid epidemic in the United States, and the sale of stolen credit card information has led to financial losses for individuals and businesses. Additionally, the anonymity provided by the darkweb has made it a breeding ground for hate speech and extremist ideologies.

XIII.Efforts to regulate and shut down the darkweb

Law enforcement agencies around the world have made efforts to shut down darkweb markets and arrest the individuals behind them. In 2013, the FBI shut down Silk Road and arrested its operator, Ross Ulbricht. In 2017, the

Dutch police shut down the darkweb market AlphaBay. Furthermore, the US government passed the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), which makes it a federal crime to operate a website that facilitates prostitution.

XIV. Current state and future trends

Despite efforts to shut down darkweb markets, they continue to exist and new ones are constantly being created. The darkweb is also becoming increasingly decentralized, with decentralized marketplaces and peer-to-peer networks making it more difficult for law enforcement to shut them down. Additionally, the anonymity provided by the darkweb is being used for legitimate purposes such as whistle-blowing and political activism.

XV. Ethical and moral issues

The use of the darkweb raises several ethical and moral issues. The anonymity provided by the darkweb can be used to protect human rights and freedom of speech, but it also allows for the sale of illegal drugs and weapons, which can harm individuals and society as a whole. Additionally, the use of the darkweb for illegal activities raises questions about personal responsibility and accountability.

XVI. Conclusion

The dark web is a complex and multifaceted ecosystem, which has both legitimate and illegitimate uses. Understanding the different components of the dark web, as well as the methods used to attack and defend anonymity on the dark web, is crucial for both individuals and organizations. Additionally, the use of dark web crawlers and data mining on the dark web must be done with consideration for ethical and legal issues. And, to understand the dark web, it's important to be familiar with the jargons and legends used on the dark web.

Darkweb is a network of hidden websites and services that can only be accessed using specialized software, such as Tor. It is primarily used for illegal activities such as buying and selling drugs, firearms, and stolen credit card information. The anonymity provided by the darkwebt can be used for both good and bad purposes, and its use raises several ethical and moral issues.

Acknowledgment

I would like to express my gratitude to the researchers and experts in the field of darkweb studies whose work has served as the foundation for this review paper. Finally, I would like to acknowledge the invaluable input and feedback provided by the reviewers, whose suggestions have greatly improved the quality and accuracy of this paper.

References

- BestVPN. (2021). The Best VPNs for TOR: Protect Your Privacy on the Dark Web. BestVPN.
- Cresci, S. (2015). How the DarkWeb is used for cybercrime. The Guardian.
- D’Angelo, J. (2016). Inside the DarkWeb: A Tour of the Underground Internet. Rolling Stone.
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium (pp. 303-320).
- Eckersley, P. (2010). How unique is your web browser? Electronic Frontier Foundation.
- Europol. (2017). Internet Organised Crime Threat Assessment (IOCTA) 2017. Europol.
- Kshetri, N. (2018). The dark side of the Internet: the criminal exploitation of the dark web. Journal of Cybersecurity, 4(2), 83-99.
- Murdoch, S. J., & Danezis, G. (2007).
- "Darknet Markets." Europol, European Union Agency for Law Enforcement Cooperation, 2020.
- "Silk Road." The New York Times, The New York Times.
- "Shutting Down AlphaBay, the World's Largest Criminal Marketplace on the Darknet." Europol, European Union Agency for Law Enforcement Cooperation, 2017.
- "Allow States and Victims to Fight Online Sex Trafficking Act of 2017." Congress.gov, Library of Congress.
- "Darknet and Bitcoin." In Bitcoin and Cryptocurrency Technologies, edited by Arvind Narayanan et al., Princeton University Press.
- "On the Underground Economy and Its Relationship to the Cybercrime Ecosystem." In Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats, edited by Sean E. Sawyer et al., Springer, 2015.
- "The Ethics of Anonymity." In The Oxford Handbook of Information Ethics, edited by Luciano Floridi, Oxford University Press, 2011.