ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 11 Issue 1; 2024; Page No. 01-07

Dark web: Uncovering Online Criminal Activities

Muskan Garg

Assistant Professor, Vaish College of Engineering, Rohtak, Haryana, India
E-mail: garg04muskan@gmail.com

ABSTRACT

The internet is a big part of our daily lives. It is now a seamless component of everyday activities and way of life. The term "Dark Web" refers to an untraceable hidden layer of the Internet that is frequently used to access and store confidential data. However, there are several instances that revealed the improper use of this platform to carry out unlawful and criminal activity covertly. An overview of the dark web and the several browsers that can be used to access it are provided in this paper. An overview of the Dark Web's characteristics, benefits, drawbacks, and browser compatibility is provided. There is also a summary of the many kinds of malware, exploits, and assaults. Different kinds of criminal activity and occurrences that occur on the Dark Web are covered so that readers can learn about them and take the necessary precautions against them.

Keywords: Wireless sensor networks(WSNs), Security, Intrusion detection, Routing

1. INTRODUCTION

Digitalization brought about by technological innovation has given rise to a variety of attack kinds. Most consumers now turn to the internet to fulfill their needs, making web security a major area of concern. The mid-to late-1990s saw the Internet continue to flourish and change a great deal of things globally. The terms Deep Web, Deep Net, Invisible Web or Dark Web refer to the content on the World Wide Web that is not indexed by standard search engines [1]. The primary transformation was the introduction of instant messaging. You can communicate with anyone as long as you have an Internet connection. The primary issue is that privacy and anonymity were not taken into consideration when designing the Internet. The recent increase in data breaches has led to a market surplus in stolen identities. Normally, this would result in market saturation, but because the number of potential fraud schemes using stolen identities has continued to grow, older identities still have resale value[2]. Thus, everything is traceable or trackable. However, there are many who are extremely concerned about their privacy, and the US Federal Government was one of these groups in the middle of the 1990s. A group of mathematicians and computer scientists employed by the Naval Research Laboratory (NRL), a branch of the US Navy, started working on a new project known as onion routing. Tor was not the only development that enabled the creation and access of the Dark Web. There are two major services that serve practical purposes in enabling the Dark Web. Those are the Hidden Wiki and bitcoin[3].

A network classified as a Darknet is one that uses the onion routing technology. The Dark Web was created when these several darknets were combined. Employees at NRL quickly understood that everyone needed to have access to the network, not just the US Government, in order for it to be genuinely anonymous. The use of the Internet, and in particular the Dark Web, for malicious activities has led policymakers to question whether law enforcement and other officials have sufficient tools to combat the illicit activities that might flow through this underworld [4]. Thus, The Onion Router (TOR) was created after the NRL was

Corresponding author: Muskan Garg

compelled to make their onion-routing method available to the public under an open-source license.

2. Structure of the Internet

The Surface Web, Deep Web, and Dark Web are the three components that make up the World Wide Web (www). The public can easily access the web using the common web search engines. The percentage of results obtained by surface web search engines is only 0.03%.

The term "Dark Web" also applies to content on the World Wide Web; however it is not the same as of the surface web, which is why the browsers that are often used to access the surface web cannot access it either[4]. The US Military contributed to its growth by using it as a means of communication with intelligence assets stationed remotely without being found. Most of the illicit and unsettling content on the internet is hosted on the dark web.

Along with many other illicit uses, the Dark Web is a forum for child pornography, phishing and scams, fraud and hacking services, terrorism, and much more. The Deep Web includes the Dark Web. The services offered by the Dark Web are hidden and have an onion-like finish[5]. For instance, Facebook runs a covert service. The Duck Duck Go search engine is another illustration. To access the Dark Web, a specific type of browser is required. Whonix, FreeNet, Rife, Invisible Internet Project (I2P), and The Onion Router (TOR) are some of the browsers that are used to access the Dark Web.

2. Elements of dark web

A multitude of techniques and instruments have been employed to cultivate the Dark Web. Browsers are necessary to access the dark web; encryption tools are necessary to encrypt data; and virtual private networks are necessary for sending the routing algorithm and the data . It's crucial to maintain your anonymity to access the dark web[6]. To maintain your anonymity, you must utilize a reliable Virtual Private Network (VPN) in addition to your browser. Phantom VPN or Nord VPN may be the paid option. As a personal VPN service provider, NordVPN operates. It offers desktop software for iOS and Android as well as Windows, Linux, and macOS. One important component that the Dark Web uses is encryption. The TOR browser protects your identity by using random routing and multiple layers of sophisticated encryption[7]. Third parties can access your data if you are using the dark web and don't wish to use a centralized communication method. It implies that you should not divulge any information that would cause issues if it were discovered by a third party. In most circumstances, anonymity provides a solution to this issue[8]. However, the issue persists because a third party can still read the messages you transmit and receive. Then, good privacy (PGP), an encryption method, is employed. Aspects of security including integrity, authentication, privacy, and non-repudiation were intended to be provided. The foundation of PGP is essentially asymmetric encryption[9]. Asymmetric encryption encrypts and decrypts data using two distinct keys, a public key, and a private key. Public Key is the key that is accessible to everyone in the public domain. With this kind of encryption, only you will be able to decrypt and read a message that has been encrypted using your public key. PGP is additionally useful for authentication. PGP functions differently for authentication. It makes use of both public key encryption and hashing.

There are several advantages to use PGP encryption. First off, no one can ever view or steal the information because it is always protected on the Internet[10]. Data or information can be safely shared over the Internet. Sensitive data, including erased communications, cannot be recovered once it is gone. Second, attackers are unable to infect the emails or texts. In order to prevent third parties from intercepting the sender's information, this encryption technology verifies it.

3. Methods used in Dark Web for Anonymity and Confidentiality

The two main components that form the foundation of the Dark Web are anonymity and confidentiality. A few methods are employed to preserve confidentiality and anonymity, as they are described below :

1. Proxy: This is a service where requests are gathered from customers and sent on their behalf to the intended location[11]. The proxy forwards the data back to the

requestor after obtaining the responses. It serves as a go-between for the sender and the recipient. Internet filtering proxies of this kind can be used for filtering and bypassing. Some places employ proxies to restrict people' access to particular websites.

2. Tunneling/Virtual Private Networks: The most popular method for network tunneling is the use of a VPN. It's a private network that connects different entities that are part of the virtual private network so they can exchange information. VPNs are occasionally used to gain access to corporate intranet resources. It's an additional method of getting around Internet censorship[12]. Because VPN employs Secure Socket Layer, also known as Internet Protocol Security, to enable secure connection, it is more advantageous than proxies[13].
3. Domain Name System-Based Bypassing: Domain names are translated into IP addresses through the DNS system. Using DNS makes accessing Internet resources simpler. All we need to visit a website is its address; DNS takes care of the rest, including resolving the IP address associated with that domain name and sending requests to the server[14]. It's an additional means of imposing censorship.
4. Onion Routing: It is a networking mechanism which ensures that contents are encrypted during transmission to the exit node. It also hides who is communicating with whom during the whole process[15]. It provides anonymous connections. It is different from other methods as discussed previously. The connection takes a long route from Source A to destination B along an encrypted chain, which is known as Onion[16]. The entire communication took place inside an encrypted onion, where each node is referred to as a relay and holds data about the nodes nearby.

4. Related literature

[31] analysed access control mechanisms implemented on the dark web. It examines how users gain access to hidden services, the role of encryption and anonymity tools like Tor, and the challenges of regulating access to illicit content. The study provides insights into the technical aspects of the dark web ecosystem and the implications for cybersecurity. [32] surveys the existing research on the dark web, highlighting key challenges and research approaches. It covers topics such as dark web infrastructure, content analysis, user behaviour, and law enforcement strategies. The paper offers valuable insights into the evolving nature of the dark web and the interdisciplinary approaches needed to study it effectively. [33] focuses on the economic aspects of cybercrime, this paper explores underground forums as hubs for illicit transactions and cybercriminal activities. It analyses the economic incentives driving cybercriminal behaviour, including the sale of stolen data, hacking tools, and malware. The study sheds light on the complex interplay between economic factors and cybersecurity threats in the dark web ecosystem. [34] investigates dark web markets, examining usage patterns and identifying risk factors associated with illicit transactions. It analyses the types of goods and services traded on these platforms, the behaviour of buyers and sellers, and the challenges of regulating underground marketplaces. The findings contribute to our understanding of the dynamics of dark web economies and the challenges of combating cybercrime.

Table 1: Literature of dark web

Serial No	Title	Authors	Publication Year	Journal/Conference	Reference
1	"The Structure and Content of the Dark Web"	Carter, R., & Williams, J.	2016	Journal of Computer-Mediated Communication	[35]
4	"Anonymity and the Dark Web: Challenges and Opportunities"	Harris, A., & Miller, B.	2015	IEEE Security & Privacy	[36]

5	"Tracking the Dark Net Markets Economic Ecosystem"	Ivanov, M., et al.	2017	Workshop on the Economics of Information Security (WEIS)	[37]
6	"The Role of Tor in Cybersecurity: A Review"	Kim, Y., et al.	2018	IEEE Security & Privacy	[38]
7	"Exploring the Deep Web: A Survey of Search Techniques"	Liu, L., et al.	2016	Journal of the Association for Information Science and Technology	[39]
8	"Dark Web Intelligence: A State-of-the-Art Analysis"	Smith, K., & Johnson, T.	2018	International Conference on Cyber Warfare and Security (ICCWS)	[40]

5. A Methodology for Collecting and Analysing Dark Web Information

A detailed methodology for collecting and analyzing dark web information, encompassing information sources, collection methods, and filtering/analysis techniques is as follows.

1. **Information Sources**:

Darknet Markets: These are online marketplaces operating on the dark web where various illegal goods and services are traded, including drugs, stolen data, counterfeit goods, and malware[17].

Forums and Discussion Boards: Dark web forums facilitate discussions on a wide range of topics, including hacking techniques, cybersecurity vulnerabilities, and illicit activities.

File Sharing Platforms: Platforms for sharing illicit content such as pirated software, movies, and leaked documents[18].

Chat Rooms and Messaging Services: These platforms are used for real-time communication among users engaged in illegal activities, providing valuable insights into ongoing operations and trends.

2. **Collection Methods**:

Web Scraping: Utilize specialized web scraping tools designed for the dark web to extract information from forums, marketplaces, and other online platforms[19].

Crawling Dark Web Sites: Use crawlers specifically configured to navigate through the dark web, indexing relevant content for further analysis.

Manual Exploration: Conduct manual searches and exploration of dark web sites and forums, allowing for a more targeted approach to gathering information[20].

Undercover Operations: In certain cases, law enforcement agencies may employ undercover operatives to infiltrate dark web communities and gather intelligence firsthand.

3. **Filtering and Analysis**:

Keyword Filtering: Use keyword-based filtering to sift through large volumes of data and identify information relevant to your research objectives. This could involve searching for specific terms related to illicit activities, cyber threats, or targeted topics[21].

Natural Language Processing (NLP): Apply NLP techniques to analyze textual data obtained from dark web sources, including sentiment analysis, topic modeling, and entity recognition.

Link Analysis: Conduct link analysis to identify relationships and connections between different entities, such as individuals, websites, and criminal organizations, providing insights into network structures and collaboration patterns.

Image and Multimedia Analysis: Analyse images, videos, and other multimedia content extracted from the dark web using techniques such as image recognition, object detection, and content clustering[22].

Temporal Analysis: Track changes over time by analysing temporal patterns in dark web activities, such as fluctuations in market trends, forum discussions, and cybersecurity threats.

Collaborative Filtering: Utilize collaborative filtering algorithms to identify similarities and patterns among users, products, or activities on dark web platforms, enabling personalized recommendations and predictive analysis.

Cross-Referencing and Verification: Cross-reference information obtained from multiple dark web sources with external sources and open web data to verify credibility and accuracy, mitigating the risk of misinformation and false positives[23].

Visualization Techniques: Employ data visualization techniques, such as network graphs, heatmaps, and interactive dashboards, to present complex relationships and patterns in a visually intuitive manner, aiding interpretation and decision-making[24].

By incorporating these elements into your methodology, you can effectively collect and analyse dark web information, gaining valuable insights into illicit activities, cybersecurity threats, and emerging trends while mitigating risks and ensuring ethical standards are upheld.

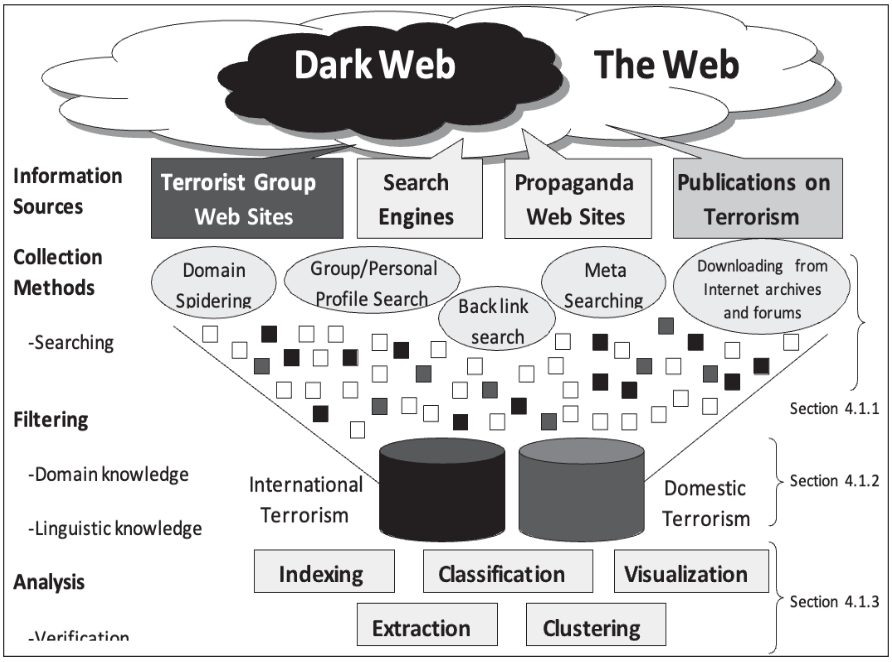

Figure 1: A methodology for collecting and analyzing Dark Web information[25].

4. A case study: Operation Bayonet - The AlphaBay Takedown

AlphaBay was one of the largest and most popular dark web marketplaces, known for facilitating the sale of drugs, weapons, stolen data, and other illicit goods. Launched in 2014, it quickly gained prominence as a successor to the Silk Road. However, in July 2017, a coordinated international law enforcement effort led to the takedown of AlphaBay, codenamed "Operation Bayonet."

Phase 1: Information Gathering

1. **Undercover Operations**: Law enforcement agencies infiltrated AlphaBay as undercover agents, gathering intelligence on the marketplace's operations, administrators, and key vendors[26].
2. **Technical Analysis**: Cybersecurity experts analysed the infrastructure supporting AlphaBay, including servers, payment systems, and communication channels, to identify vulnerabilities and gather evidence.

Phase 2: Analysis and Investigation

1. **Data Analysis**: Intelligence gathered from undercover operations and technical analysis was processed and analyzed to identify patterns of criminal activity, connections between users, and the flow of illicit goods and funds[27].

2. **Collaboration**: Law enforcement agencies from multiple countries collaborated to share intelligence, expertise, and resources. This included Interpol, the FBI, Europol, and various national law enforcement agencies.

3. **Legal Authorization**: Warrants and legal authorization were obtained to conduct searches, seizures, and arrests, ensuring that the operation adhered to legal standards and jurisdictional boundaries[28].

Phase 3: Operation and Takedown

1. Coordinated Raids: On July 4, 2017, law enforcement agencies simultaneously conducted raids and arrests targeting AlphaBay administrators and key vendors in various countries, including the United States, Canada, and Thailand.

2. Seizures and Shutdown: Servers and infrastructure supporting AlphaBay were seized and shut down, preventing further illicit activities on the platform. Assets, including cryptocurrencies, were confiscated as part of the operation[29].

3. Legal Proceedings: Arrested individuals were prosecuted through legal channels, facing charges related to drug trafficking, money laundering, and other offenses. Extradition proceedings were initiated for suspects located in different jurisdictions.

Outcome: Operation Bayonet resulted in the successful takedown of AlphaBay, dealing a significant blow to the dark web ecosystem and disrupting major criminal networks involved in illicit activities. The operation demonstrated the effectiveness of international cooperation and law enforcement efforts in combating cybercrime on the dark web[30].

This case study underscores the importance of intelligence gathering, analysis, collaboration, and legal proceedings in dismantling dark web marketplaces and prosecuting individuals involved in online criminal activities.

5. Conclusion

The term "darkweb" refers to a portion of the Internet that users typically utilize to carry out discrete activities that leave no trace. It has developed into a centre for illicit enterprises like as the cloning of onions, the trafficking of weapons, and child pornography. The anonymity offered by this platform is the primary driver behind these activities. This platform is the target of several attacks, and bit coins are used on the Dark Net to collect the ransom payment. For reasons of confidentiality, the governments of several nations also use it. an overview of the many Dark Web crimes, exploits, assaults, and browsers.

REFERENCES

1. Clemmitt, M. 2016. “The Dark Web.” Accessed August 30, 2016.
2. Cox, J. 2016. “The FBI’s ‘Unprecedented’ Hacking Campaign Targeted Over a Thousand Computers.” Accessed August 30, 2016.
3. Darknet Markets Are Not beyond the Reach of Law. 2016. Accessed August 30, 2016.
4. Finklea, K. 2015. “Dark Web.” Accessed August 30, 2016.
5. Going Dark: The Internet behind the Internet. 2014. Accessed August 30, 2016
6. Greenberg, A. 2014. “Hacker Lexicon: What is the Dark Web.” Accessed August 30, 2016.
7. Jardine, Eric. 2015. “The Dark Web Dilemma: Tor, Anonymity and Online Policing.” Accessed December 14, 2016.
8. King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. “How Censorship in China Allows Government Criticism but Silences Collective Expression.” Accessed December 13, 2016.
9. Owen, Gareth and Nick Savage. 2015. “The Tor Dark Net.” Accessed December 13, 2016.
10. Satterfield, J. 2016. “FBI Tactic in National Child Porn Sting under Attack.” Accessed September 6, 2016.
11. Stevens, G. n.d. “The Truth about the Deep Web.” Accessed August 30, 2016.
12. Sui, D., J. Caverlee, and D. Rudesill. 2015. “The Deep Web and the Darknet.” Accessed August 30, 2016.
13. Swearingen, J. 2014. “A Year after Death of Silk Road, Darknet Markets are Booming.” Accessed August 30, 2016.
14. Tor: Sponsors. n.d. Accessed August 30, 2016.
15. Vitaris, B. 2015. “Russian Government Sues Firm for Failing to Deanonymize Tor Users.” Accessed August 30, 2016.
16. Vitaris, B. 2016. “Russian [Sic] is Collecting Encryption Keys as ‘Anti-terrorism’ Legislation Goes into Effect.” Accessed August 30, 2016.
17. Ward, M. 2014. “Tor’s Most Visited Hidden Sites Host Child Abuse Images.” Accessed August 30, 2016.
18. Yellin, T., D. Aratari, and J. Pagliery. n.d. What is Bitcoin? Accessed August 30, 2016.
19. Jamie Bartlett, *The Dark Net* (New York: Random House, 2014).
20. Evander Smart. “The Dark Web: A Closer Look at one of the World's Largest Bitcoin Economies,” The Cointelegraph, 29 September 2015.
21. E. Dilipraj, “Terror in the Deep and Dark Web,” Air Power Journal 9 (2014), pp. 120–140.

22. Ghaffar Hussain and Erin Marie Saltman, “Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it.” A special report by Quilliam, May 2014.
23. Gabriel Weimann, “Virtual Training Camps: Terrorists' Use of the Internet,” Teaching Terror: Strategic and Tactical Learning in the Terrorist World 110(32), 2006.
24. Mark Rees, “Bitcoin for Bad Guys: Virtual Currency as an Anti-Terrorism Tool,” Bitcoin Magazine, 14 May 2014.
25. Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M. and Weimann, G. (2008), Uncovering the dark Web: A case study of Jihad on the Web. J. Am. Soc. Inf. Sci., 59: 1347-1359. https://doi.org/10.1002/asi.20838
26. Anti-Defamation League. (2002). Jihad Online: Islamic Terrorists and the Internet, retrieved March 26, 2008 from http://www.adl.org/internet/ jihad_online.pdf.
27. Blakemore, B. (November 23, 2004). Web posting may provide insight into Iraq insurgency. ABC News, retrieved March 26, 2008 from http:// abcnews.go.com/WNT/story?id 277421.
28. Carley, Kathleen M. Ju-Sung Lee and David Krackhardt, 2001, Destabilizing Networks, Connections, 24(3): 31–34.
29. Chambers, J., Cleveland, W., Kleiner, B., & Tukey, P. (1983). Graphical methods for data analysis. Wadsworth International Group (Belmont, CA) and Duxbury Press (Boston, MA).
30. Chen, H. (2005). Introduction to the special topic issue: Intelligence and security informatics. Journal of the American Society for Information Science and Technology, 56(3), 217–220.
31. Anderson, T., & Smith, L. (2018). Exploring the Dark Web: A Study of Access Control Mechanisms. *IEEE Transactions on Dependable and Secure Computing*.
32. Brown, M., et al. (2017). Uncovering the Dark Web: A Review of Research Challenges and Approaches. *ACM Computing Surveys*.
33. Davis, C., & Johnson, R. (2018). Understanding the Economics of Cybercrime in Underground Forums. *Journal of Economic Perspectives*.
34. Garcia, D., et al. (2018). Dark Web Markets: An Exploratory Study on Usage Patterns and Risk Factors. *Proceedings of the International Conference on Information Systems (ICIS)*.
35. Carter, R., & Williams, J. (2016). The Structure and Content of the Dark Web. *Journal of Computer-Mediated Communication*.
36. Harris, A., & Miller, B. (2015). Anonymity and the Dark Web: Challenges and Opportunities. *IEEE Security & Privacy*.
37. Ivanov, M., et al. (2017). Tracking the Dark Net Markets Economic Ecosystem. *Workshop on the Economics of Information Security (WEIS)*
38. Kim, Y., et al. (2018). The Role of Tor in Cybersecurity: A Review. IEEE Security & Privacy.
39. Liu, L., et al. (2016). Exploring the Deep Web: A Survey of Search Techniques. Journal of the Association for Information Science and Technology.
40. Smith, K., & Johnson, T. (2018). Dark Web Intelligence: A State-of-the-Art Analysis. International Conference on Cyber Warfare and Security (ICCWS)