Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

A Critical Study on Awareness on dark web

M. Ugarthi Shankalia

Assistant Professor
School of Law
Sathyabama Institute of Science and Technology
Chennai

Abstract
The dark web is the World Wide Web content that exists on dark nets, overlay networks that use the Internet but require specific software, configuration or authorisation to access. It is a part of the web that is not easily accessible and is not indexed by the search engines. It is a subset of deep web that is intentionally hidden and requires a specific browser Tor to access. It is a network of sites with encrypted content, accessible only with the secure browser tools. The software encrypts user traffic and passes the IP address through the complex software nodes. The dark web or dark net was first discovered by the United States government in order to allow spies to exchange information completely anonymously and the tor was developed in the mid 1990s by the US military researchers. The main objective of the research is to create an awareness on what is dark web and for what purposes it is being used for. An empirical method is approached for this research and a convenient sampling method is used. The total number of responses collected for the study is 193. The results observed from the analysis done is that the dark web is the main reason for the happenings of cybercrime and the black market activities mainly happen on dark web sites.

Key words
Dark web, Encryptions, Configuration, Internet Protocol and Technological improvements.

1. Introduction

The dark web is depicted as the segment which in general is described as the hidden web page that any normal person or layman cannot have easy access to. The users can access the dark web with an expectation that they are able to share the information and the file without having a little risk of detection. The dark web refers to the assortment of websites which is present on an encrypted network and cannot be accessed by utilising the conventional search engines or browsers. Almost the entire websites on dark web on dark web conceal their identities by utilising the tor encryption as it is capable of hiding the identity of the websites as well as the activities that are being performed in them. The dark web is defined as the particular subsection which is related to a collection of websites. This process is continuing the hiding of IP (Internet protocol) address and the server process is not detectable since there is an encryption being used to show the anonymity. of the dark web is dynamically produced by the web server as well as a return to the users throughout the online query. In order to access the dark Web the users should request from a particular database through a search interface.

Currently this observed that a large amount of data on the WWW is obtainable only through the search interface. The unprecedented growth of the Internet has given rise to the dark web. Many recent studies have shown how terrorists use the web to facilitate their activities. The hackers are also using the dark web to expose or sell the data and information causing damage to the organisation and individuals. On the other hand the dark web has been criticised for conducting cybercrime such as drug trafficking, child trafficking, cyber terrorism etc. The dark web sites serve as a platform for internet users for whom anonymity is essential since they not only provide protection from unauthorised users but also usually include encryption to prevent monitoring. The ability to traverse the internet with complete anonymity nurtures a platform for the considered illegal activities including controlled substance marketplaces, credit card fraud and identity theft and leaks of Sensitive information.

Many websites such as Silk Road act as anonymous marketplaces selling Things that are elicit such as drugs and weapons. The dark web in general and the tor network in particular offer a secure platform for cyber criminals which support a past amount of illegal activities. As such it has become increasingly important for security agencies to track and monitor the activities in the dark web, focusing today on the tor networks but possibly extending to other technologies in the near future the lack of observable activities in unconventional dark web networks does not mean they do not exist. In fact in agreement with the principle that inspires the dark web, the activities are simply more difficult to spot and observe. This becomes the driving factor for the dark web to operate at a higher position.

2. Objectives

- To determine whether the dark web is the main reason for criminal activities.
- To determine whether the dark web is the major source for black market activities.

3. Review of literature

The Internet has evolved to become a global platform through which anyone can conveniently disseminate, share, and communicate ideas. Despite many advantages, misuse of the Internet has become ever more serious, however. Terrorist organizations, extremist groups, hate groups, and racial supremacy groups are using the Web to promote their ideology, to facilitate internal communications, to attack their enemies, and to conduct criminal activities(Gehl, 2016) . Warnings have been made that terrorists may launch attacks on such critical infrastructure as major e-commerce sites and governmental networks(Jardine, 2018) . As the Web grows larger and more diverse, search engines are becoming the “killer app” of the Web. Whenever users want to look up information, they typically go to a search engine, issue queries and look at the results. Recent studies confirm the growing importance of search engines (Jeffrey, 2012). According to Nielsen for example, Web users spend a total of 13 million hours per month interacting with Google alone. For the purpose of providing comprehensive characteristics, the forum of the dark web is constructed with the various sources of the data in a sequential and the timely manner (Chen, 2011). This helps in the arrangement of the data, and thereby the appropriate collection process can be continued by the users. Therefore, the accessibility and the collection update issues can be easily removed while depicting the important characteristics(Ozkaya & Islam, 2019) .

The impact of the social interactions is widely depicted by the usage of the social networks, and thereby the real world networks can be easily identified. The social networks are formed by the usage of the Dark

networks which are crucial for building the sites of the social networking. The Dark networks are either real or virtual, and thereby the criminal activities can be conducted in an easy way (Amores & Paganini, 2012). Focused crawlers are defined as seek, index, maintain and acquire pages on a specific topic that represents the narrow segment of the web. The need to gather high quality, specific domain contents results in significant characteristics for the crawlers that are relevant for the collection of the Dark Web forums (Robertson et al., n.d.). The dark web, also known as darknets or hidden services, is a subset of the network not indexed by search engines because it requires the use of special software for access(Chertoff, 2017) . It consists of both public and private elements, accessible publicly or by only those with credentials provided the correct software is in use. The key difference between the dark web and surface or deep web lies in the lack of accountability present on the dark web (Koch & Rodosek, 2016). Users are unidentifiable to the network or anyone monitoring and their actions are thus effectively anonymised (Henderson, 2015).

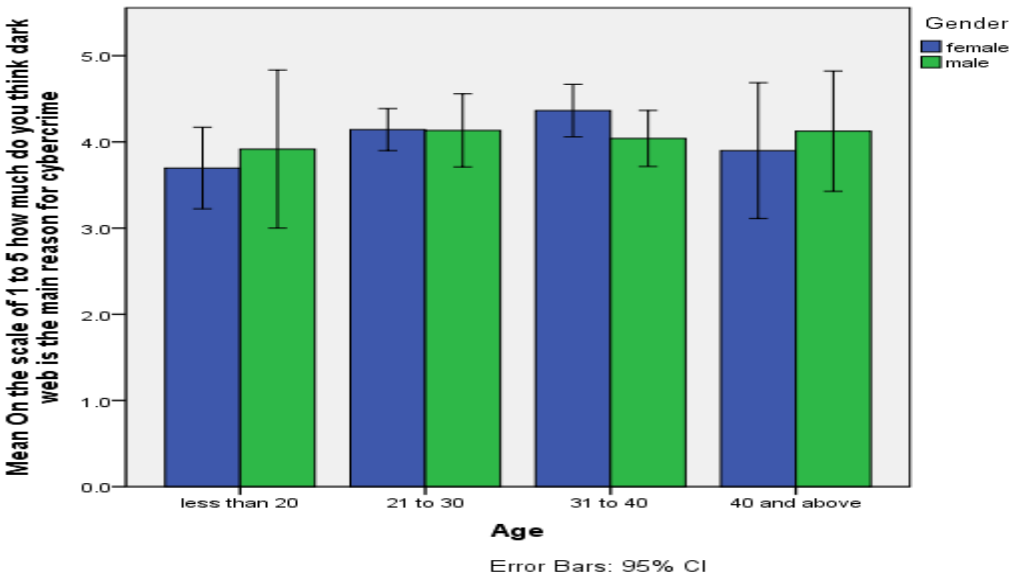
Furthermore, the dark web allows for hosting of web services (hidden services) which remain anonymous with regards to their true IP address, and thus location, even to the users who use those web services (Moallem, 2019). The difference thus between the dark and deep web is that the former is characterised by unique technology-enabled protocols and anonymity, whereas the latter is more reliant on authentication and thus a lack of public access (Khosrow-Pour, 2020). Anonymity is not a feature of the deep, and surface, web and both have their unauthenticated parts readily indexed by search engines. By conferring anonymity, private engagements between people have been institutionalised by the dark web (Retzkin, 2018). The dark web is a feature of specific overlay distributed systems that exist atop the global internet (Liggett et al., 2020). These networks provide the functionality of remaining untraceable and promise to be a haven from prying eyes, mainly law enforcement . Multiple avenues making this promise have existed over the years, and some have been temporary in their popularity and even operation(Croy, 2018). Technological improvements have allowed for novel ways to enable the dark web to exist and sustain itself longer than before. It is possible that the current generation of tools and networks in use will outlive their predecessors as they learn from their failures and improve upon them(Senker, 2016).

The most prominent manifestation of the dark web the Tor network works by routing internet traffic via multiple nodes, each of which is only aware of the sender and destination in their immediate vicinity and thus unaware of the original sender and destination of that traffic (Kirkpatrick, 2017). Much like the Internet, and because of it being an overlay, the dark web exists on a system which is decentralised and to an extent distributed in nature with no central servers or point of control(Villalva et al., 2018) . The promise of anonymity on the dark web opens itself up for use in multiple ways. Some legitimate reasons include civilians looking for protection from irresponsible corporations, censorship, ability to research into sensitive topics without concerns; militaries hosting hidden command and control services, journalists conducting their operations in countries without access to free media and speech; law enforcement performing sting operations, activists and whistle-blowers reporting abuses and speaking out against governments (Sinha, 2017). The dark web is not the only place for cybercrime groups to sell their skills and products. Surface web forums, including Facebook, have long been used by criminals to offload and sell their services of spamming, fraud, DoS attack-for-hire services, stolen credit card details, among others. However, being on the surface web, these avenues are ripe for easier takedowns and prosecution (Jones, 2017; Sinha, 2017).

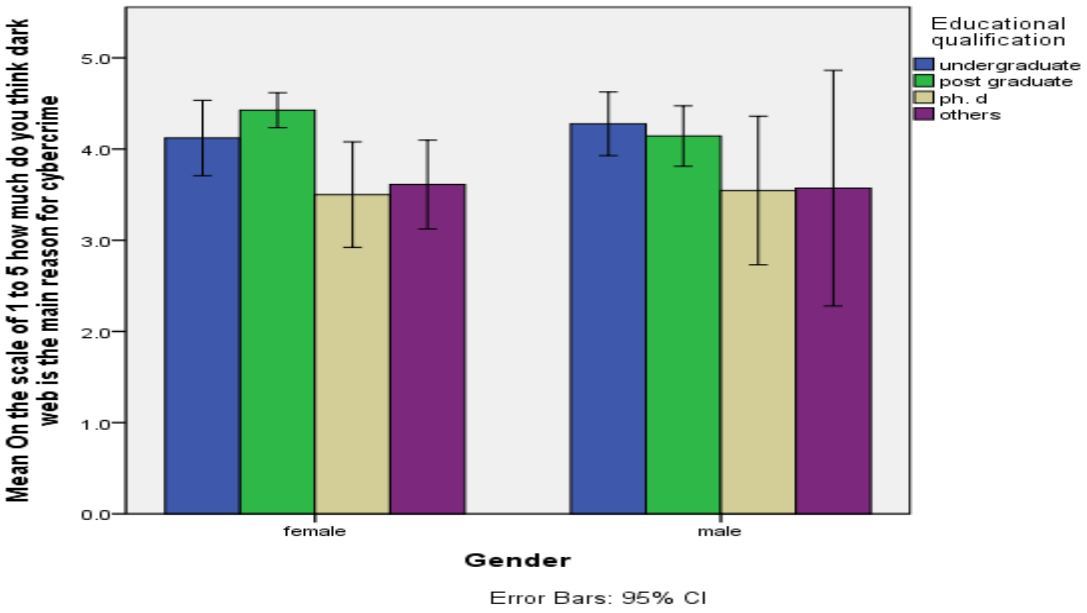
4. Methodology

Empirical research is adopted for the study. Convenience sampling method is used for the study. A sample size of 193 responses are collected with regard to the study from the general public through an online survey by asking the respondents to fill out the questionnaire. The independent variables used for the study are age, gender and educational qualification and dependent variables are awareness on the dark web and criminal activities happening on the dark web. The statistics used are graphical analysis, the Pearson correlation and spearman correlation.

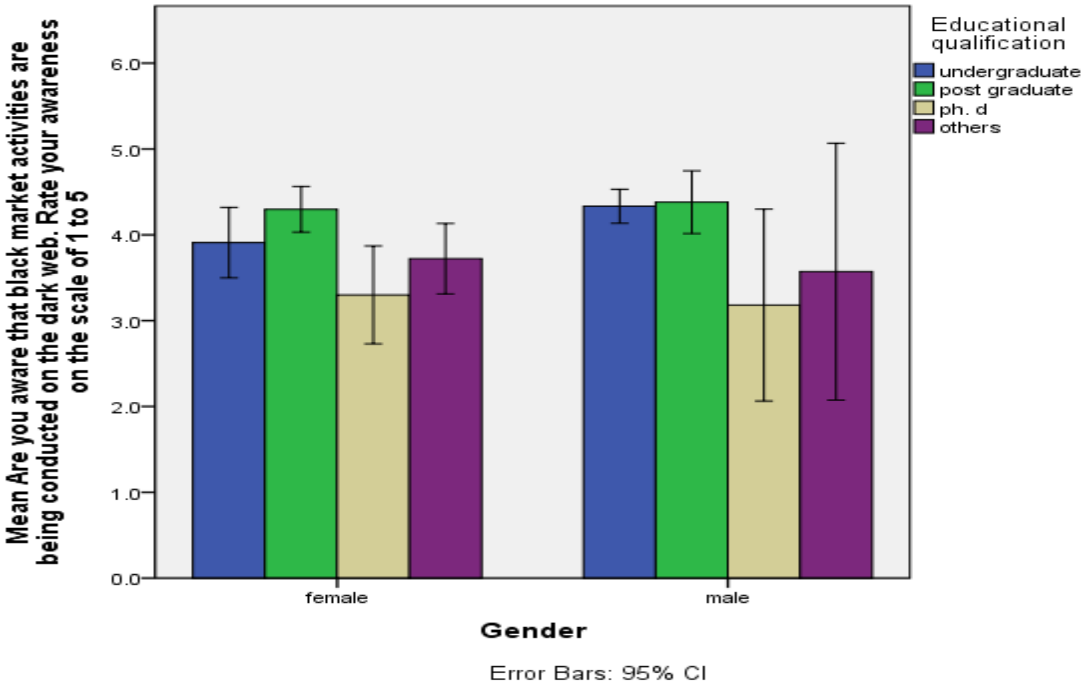
5. Analysis



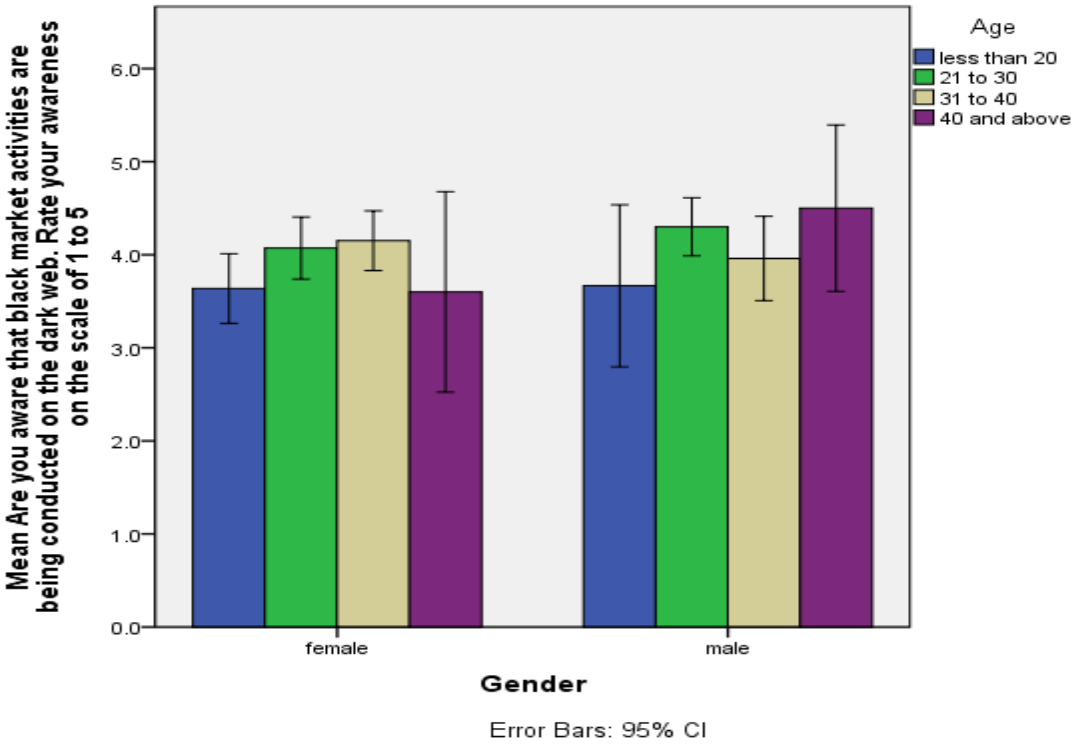
From the above graph the graphical analysis is done for the acceptance levels for the question dark web is the main reason for cybercrime corresponding to age and gender.



From the above graph the graphical analysis is done for the acceptance levels for the question dark web is the main reason for cybercrime corresponding to educational qualification and gender.



From the above graph the graphical analysis is done for the acceptance levels for the question black market activities are being conducted on dark web corresponding to educational qualification and gender.



From the above graph the graphical analysis is done for the acceptance levels for the question black market activities are being conducted on the dark web corresponding to age and gender.

6. Correlations

Hypothesis

Null hypothesis

There is no significant relationship between the dark web as a main reason for cyber crimes and black market activities conducted on dark web.

Alternate hypothesis

There is a significant relationship between the dark web as a main reason for cyber crimes and black market activities conducted on the dark web.

Descriptive Statistics

	Mean	Std. Deviation	N
On the scale of 1 to 5 how much do you think dark web is the main reason for cybercrime	4.062	1.0339	193
Are you aware that black market activities are being conducted on the dark web. Rate your awareness on the scale of 1 to 5	4.000	1.0704	193

In the above correlation table the value of mean and standard deviation for the variable dark web is the main reason for cybercrime is 4.062 and 1.0339. The mean and standard deviation for the variable black market activities being conducted on the dark web is 4.000 and 1.0704.

Correlations

		On the scale of 1 to 5 how much do you think dark web is the main reason for cybercrime	Are you aware that black market activities are being conducted on the dark web. Rate your awareness on the scale of 1 to 5
On the scale of 1 to 5 how much do you think dark web is the main reason for cybercrime	Pearson Correlation	1	.494**
	Sig. (2-tailed)		.000
	N	193	193
Are you aware that black market activities are being conducted on the dark web. Rate your awareness on the scale of 1 to 5	Pearson Correlation	.494**	1
	Sig. (2-tailed)	.000	
	N	193	193

**. Correlation is significant at the 0.01 level (2-tailed).

In the above correlation table the Pearson value is positive and falls below 0.01, this accepts the alternate hypothesis which confirms the relationship between the dark web as a main reason for cyber crimes and black market activities conducted on the dark web.

Correlations

	On the scale of 1 to 5 how much do you think dark web is the main reason for cybercrime	Are you aware that black market activities are being conducted on the dark web. Rate your awareness on

				the scale of 1 to 5
Spearman's rho	On the scale of 1 to 5 how much do you think dark web is the main reason for cybercrime	Correlation Coefficient Sig. (2-tailed) N	1.000 . 193	.277** .000 193
	Are you aware that black market activities are being conducted on the dark web. Rate your awareness on the scale of 1 to 5	Correlation Coefficient Sig. (2-tailed) N	.277** .000 193	1.000 . 193

**. Correlation is significant at the 0.01 level (2-tailed).

In the above correlation table the spearman's value is positive and falls below 0.01, this accepts the alternate hypothesis which confirms the relationship between the dark web as a main reason for cyber crimes and black market activities conducted on the dark web.

7. Results

From graph 1 majority of the respondents who belong to the gender category females at age category 31 to 40 have given higher acceptance that dark web is the main reason for cybercrime. And the Male respondents belonging to the age group 40 and above have given higher acceptance that dark web is the main reason for cybercrime. In the graph the majority of the female respondents who belong to postgraduate educational qualification have given higher acceptance to the question dark web is the main reason for cyber crimes. And the undergraduate educational qualification belonging to the male category had given higher acceptance to the same. From the graph three majority of the male and female respondents both belonging to the Post graduate educational qualification have said that black market activities are being conducted on the dark web. In the graph 4 Majority of the male respondents of above 40 age category have given higher acceptance that Market activities are being conducted on the dark web. And majority of the female respondents belonging to the age group 31 to 40 have given higher acceptance to the same.

8. Discussions

Based on the results, we can state the following dark web is the main reason for the majority of the cybercrime and the direction of relationships is positive which confirms that there is a significant relationship between the dependent variables which confirms the alternate hypothesis from the Pearson value given. And from the analysis done by the spearman's correlation also the respondents have answered that black market activities are mostly conducted on the dark web. This also gives a positive approach which confirms that there is a significant relationship between the dependent variables and the alternate hypothesis is accepted. The same can be viewed from the graphs also where in graph one majority of the respondents have answered that darkweb is the main reason for the happenings of cyber crimes. In graph two most of the female respondents have accepted that most of the cybercrime activities take place because of the dark web. And the respondents belonging to PhD educational qualification have relatively given

lower acceptance for the statement cybercrime activities mostly happen on the dark web. In the graph three majority of the male and female respondents belonging to the post graduate educational qualification have given higher rates of acceptance to the dark web as the main sources where black market activities are happening. Whereas the respondents belonging to the PhD educational qualification have relatedly given lesser agreeability to the statement. In graph 4 the opinion of the 40 and above males have said that black market activities are being conducted on the dark web.

9. Conclusion

From the graphical analysis, correlation analysis and the Pearson correlation and spearman's correlation values obtained in the study the alternate hypothesis is accepted which confirms that the dark web is the main reason for the happenings of cybercrime and the black market activities mainly happen on dark web sites. The proven hypothesis shows that there is a significant relationship between the dark web and cybercrime and black market activities happening on dark web.

References

1. Amores, R. G., & Paganini, P. (2012). The Deep Dark Web: The Hidden World. Createspace Independent Pub.
2. Chen, H. (2011). Dark Web: Exploring and Mining the Dark Side of the Web. In 2011 European Intelligence and Security Informatics Conference. https://doi.org/10.1109/eisic.2011.78
3. Chertoff, M. (2017). A public policy perspective of the Dark Web. In Journal of Cyber Policy (Vol. 2, Issue 1, pp. 26–38). https://doi.org/10.1080/23738871.2017.1298643
4. Croy, A. (2018). The Dark Web: The Covert World of Cybercrime. Greenhaven Publishing LLC.
5. Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. In New Media & Society (Vol. 18, Issue 7, pp. 1219–1235). https://doi.org/10.1177/1461444814554900
6. Henderson, L. (2015). Tor and the Dark Art of Anonymity: How to Be Invisible from Nsa Spying. CreateSpace.
7. Jardine, E. (2018). Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. In New Media & Society (Vol. 20, Issue 8, pp. 2824–2843). https://doi.org/10.1177/1461444817733134
8. Jeffrey, S. (2012). A new Digital Dark Age? Collaborative web tools, social media and long-term preservation. In World Archaeology (Vol. 44, Issue 4, pp. 553–570). https://doi.org/10.1080/00438243.2012.737579
9. Jones, J. (2017). Hacking & Tor: The Ultimate Beginners Guide to Hacking, Tor, & Accessing the Deep Web & Dark Web. Createspace Independent Publishing Platform.
10. Khosrow-Pour, M. (2020). Encyclopedia of Criminal Activities and the Deep Web. Information Science Reference.
11. Kirkpatrick, K. (2017). Financing the dark web. In Communications of the ACM (Vol. 60, Issue 3, pp. 21–22). https://doi.org/10.1145/3037386
12. Koch, R., & Rodosek, G. (2016). ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security ". Academic Conferences and publishing limited.
13. Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). 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 (pp. 91–116). https://doi.org/10.1007/978-3-319-78440-3_17
14. Moallem, A. (2019). Cybersecurity Awareness Among Students and Faculty. CRC Press.
15. Ozkaya, E., & Islam, R. (2019). Introduction to Cybersecurity and Dark Web. In Inside the Dark Web (pp. 3–24). https://doi.org/10.1201/9780367260453-2
16. Retzkin, S. (2018). Hands-On Dark Web Analysis: Learn what goes on in the Dark Web, and how to work with it. Packt Publishing Ltd.
17. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (n.d.). Understanding Darkweb Malicious Hacker Forums. In Darkweb Cyber Threat Intelligence Mining (pp. 13–37). https://doi.org/10.1017/9781316888513.005
18. Senker, C. (2016). Cybercrime & the Dark Net: Revealing the hidden underworld of the internet. Arcturus Publishing.
19. Sinha, S. (2017). Dark Web and Tor. In Beginning Ethical Hacking with Python (pp. 173–177). https://doi.org/10.1007/978-1-4842-2541-7_26
20. Villalva, D. A. B., Onaolapo, J., Stringhini, G., & Musolesi, M. (2018). Under and over the surface: a comparison of the use of leaked account credentials in the Dark and Surface Web. In Crime Science (Vol. 7, Issue 1). https://doi.org/10.1186/s40163-018-0092-6