Role of the Dark Web Communities in Cybercriminal Operations

Akramova Marjona Oripovna
Tashkent State University of Law
akramovamarjona11@gmail.com

Abstract

Currently, the crimes, which commited through dark web are being opened and investigated by law enforcement agencies. However, cybercrimes are increasing day by day, especially, which are commited by means of Dark Web. This article provides information about the research methodology, the advantages and disadvantages of the Dark Web, additionally, the anonymity and other aspects of Dark Web in cybercriminal operations. Besides, this article answers the questions like: what Dark Web is, it is illegal to use or not, what goes on in the Dark Web and who uses it.

Moreover, it is difficult for law enforcement agencies or digital forensic professionals to pinpoint the origin of traffic, location or ownership of any computer or person on the Dark Web. The cause of this type of difficulty is also explained in the article. In this article, I proposed the challenge of Dark Web. I also considered and discussed its assumptions and why use the Dark Web and its role in cybercriminal operations.

Keywords: Dark web communities, Deep Web, Surface Web, cybercriminal operations, anonymity, shadow internet.

I. Introduction

Every day a modern person uses the services of the global Internet, which can be called Surface Web. Opening their emails, websites of various subjects or accounts, users do not realize the fact that all this is only a small part of the global network, which is called the Surface.

Before analyzing cybercrime operations, I believe it is advisable that we distinguish between Surface Web, Deep Web and Dark Web.

We consider the Internet as divided into the Surface Web and the Deep Web. The Surface Web, which is also known as the visible web is the part of the Internet that is easily accessible by anyone nother layer of the Internet is called the Deep Web. Accessing the Deep Web with search engines alone is not possible since websites located on the Deep Web are not indexed. The Deep Web contains a huge amount of data and information that is not easily accessible to the public. Take for example, an academic research paper published on a website where paying a subscription fee is required to access contents. Only subscribers are able to access this research paper, thus the fact that the paper is not publicly available makes it part of the Deep Web.

The Dark Web on the other hand is a specific part of the Deep Web that is also hidden yet is only accessible through specialized software and tools. Activities are conducted anonymously on the Dark Web, making it a shelter for criminal activities such as cybercrime and selling drugs. [2]

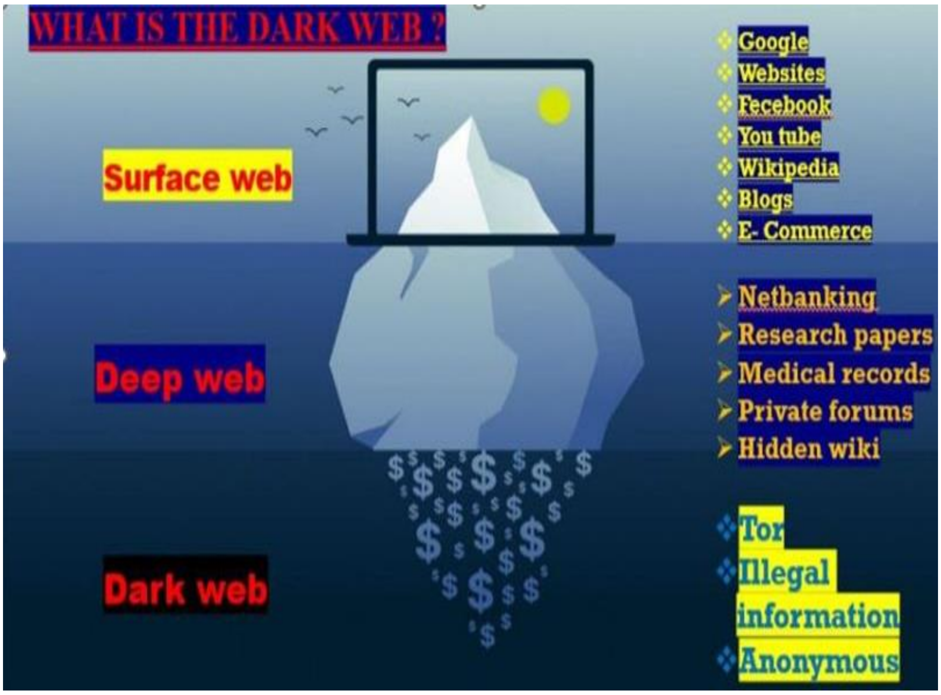
The Dark Web is a hidden part of the Internet that has gained attention due to its illegal activities and potential impact on society. [3]

I. Methodology

In this article, several sources were used to explain the importance of research topic and its essential role in cyberspace. Through methods of comparison and analysis, the essence of Dark Web, the role of this Web in cybercrime operations were learned and the research of scientists about it were analyzed. In order to reveal important aspects of the topic, various scientific articles and journals, foreign experiments, manuals were used. Also, role of the Dark Web communities in cybercriminal operations is studied from generality to specificity through observations and research, by using deduction method. Furthermore, to illustrate the findings more clearly I used some non-textual elements, like photos and tables.

II. Results

Depending on the availability of resources, the Internet can be divided into three levels, the part of which the search engines (Yandex, Google, Rambler, Bing, etc.) seem to cover is called Clear Net. Closed (conditionally closed) and web resources, called deep Internet (Deep Web), which is not indexed by search robots (crawlers) and is not indicated in search queries, occupy at least 80% of network resources, according to the authors. At the last level there is the shadow Internet (Dark Net), the sources of which can be accessed using special software (TOR, I2P, VPN. Strictly speaking, Darknet is not a component of the internet, the technology in question works on existing communication channels using similar mechanisms. [4]



What is the role of the dark web communities in cybercriminal operations?

Anonymity provided by the Dark Web serves different kinds of purposes and can facilitate illegal activities such as drug trafficking and cybercrime while also providing a platform for individuals to be able to express their thoughts freely.

Underground Marketplaces: Dark Web marketplaces make contributions to like hubs for cybercriminal activities, providing platforms for the sale and trade of stolen data, hacking tools, exploit kits, financial facts, malware, and other illegal goods and services.

Money Laundering and Cryptocurrency: The Dark Web opportunities money laundering schemes through cryptocurrency transactions, making it simle for cybercriminals to monetize their activities and evade conventional financial tracking methods.

Is the Dark Web Illegal?

Similar to using a standard web browser to access the open web, the act of using Tor or a dark web browser to access the dark web is not illegal in and of itself. It is illegal to perform illegal acts on the dark web, regardless of the level of anonymity provided by the platform.

Users of the dark web should also realize that although their activity is technically anonymous, associating with people who are conducting illegal activities can have legal implications. Several recent high-profile takedowns of Dark Web marketplaces such as Silk Road, Alpha Bay, and Wall Street Market have resulted in hundreds of arrests around the world, underscoring the risks of engaging in illegal activity in any form. Cybersecurity companies and research organizations actively monitor the dark web for cybercriminal activities. The purpose of these kind of actions is to control the rate of cybercrimes.

Products and Services on Dark Web websites
Stealing personal information services
Fake IDs
Counterfeit currency
Trojans and Malware
Organ trade (illegal organ trafficking)
DDos attacks
Weapons (firearms,ammunition)
Stolen credit cards
Drugs
Human trafficking services

III. Discussion

It is very important that we do not confuse deep web and dark web. Deep web can be accessed by anyone who has The Onion Router (TOR) browser. TOR is a virtual and encrypted tunnel which allows people to hide their identity and network traffic and allow them to use internet anonymously. Darknet was originally often associated with the Tor network, when the infamous drug bazaar Silk Road once made headlines. Anonymous communication between whistle-blowers, which is a person who exposes secretive information or activity that is deemed illegal, unethical, or not correct within a private or public organization. Journalists and news organizations is also facilitated by the "Darknet" Tor network through use of applications such as Secure Drop. [5]

Everyone may have a reasonable question that it is easy to catch up when buying products or services in Dark Web due to the control of banks. To determine cybercrimes, which are commited in forbidden zone of Internet, is very complicated because no bank cards used in Dark Web. In Dark Web, all actions are carried out using cryptocurrencies, since blockchain is a decentralized system and it is impossible to determine where crypto wallets are standing inside it. In addition to individuals, darknet is also used by the media. Since the most anonymous way to deliver data is darknet.

It should not be forgotten to mention that it is also available several benefits of Dark Web.

For better:

- to circumvent government censorship;
- to provide whistleblowers protection;
- to avoid monitoring.

Benefit sides of the dark network: The dark web helps people to maintain privacy and freely express their views. Privacy is essential for many innocent people terrorized by stalkers and other criminals. The increasing tendency of potential employers to track posts on social media can also make it difficult to engage in honest discussions publicly.

To combat Cybercrime on the Dark Web we can apply such kind of efforts, like:

- Law Enforcement;

- Informatin sharing and contribution;

- Dark Web Monitoring: Cybersecurity companies and research organizations actively monitor the Dark Web for cybercriminal activities;

- Cybersecurity Education and Consciousness: Raising awareness among organizations, individuals and businesses about the risks associated with the Dark Web and cybercrime is essential;

- Blockchain Exploration: Cryptocurrency transactions on the Dark Web can be traced through blockchain analysis.

Conclusion

As a conclusion, I can say that the illegal activities of the Dark Web can only be prevented by the following actions:

- it is necessary to better study the tools and resources used by criminals in the field of cybercrime. It should be noted that, although the Tor Browser is well studied, at the same time it is necessary to expand the knowledge about other network browsers;
- the methodology and tactics of investigating crimes in Dark Web should be developed;
- to open crimes, it is vital to direct operational people to public networks, since in most cases criminals use a closed network only as a platform for committing crimes, and the development of the client base occurs mainly on surface network;
- to avoid cybercrimes, it is significant to increase the knowledge of the population in cyber security;

- ❖ additionally, to provide information about the presence of criminal liability for cybercrime and the use of darknet;
- ❖ blockchain analysis and dark web monitoring must be improved by making new laws against cybercrime.

I came to the conclusion that, in the future it is possible to effectively deal with the illegal aspects of the Dark Web by paying attention to the above suggestions which take part in this article.

References

1. Alexandrov A. G., Safronov A. A. *The use of the Darknet network in the preparation and commission of crimes* // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2021. – № 1 (89). – Pp. 156-160; doi: 10.35750/2071-8284-2021-1-156-160 https://cyberleninka.ru/article/n/ispolzovanie-seti-darknet-pri-podgotovke-i-sovershenii-prestupleniy

2. K. Taylor, *“Detailed introduction about the surface, deep dark web levels explored,”* introduction-surface-web-deep-dark-web/, accessed 2023-06-03. https://www.hitechnectar.com/blogs/

3. Hasan Saleh. – *Beneath the Surface: Exploring the Dark Web and its Societal Impacts* // Degree project. – 2023. IT 23044.

4. Gonov Sh.Kh., Milovanov A.V. — *Topical issues of countering crime in the Darknet network* // Police and investigative activities. – 2021. – No. 1. – pp. 26-34. DOI:10.25136/2409-7810.2021.1.34560. https://nbpublish.com/library_read_article.php?id=34560

5. Zakariye Mohamud Omar, Jamaluddin Ibrahim. - *An Overview of Darknet, Rise and Challenges and Its Assumptions* // International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 8, Issue 3, pp: (110-116), Month: July - September 2020. https://www.researchpublish.com