IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

NEED FOR THE PREVENTION OF DARK WEB ACTIVITIES

Jaspreet kaur, Dr. Sunowar ameer

Student, Associate professor
Lovely professional University

,Abstract

Dark web is a part of world wide web that encompasses obscure matter which otherwise cannot be indicated by standard internet portals. The identities of users browsing the dark web remain unrevealed, implicating the consolidation of legal and illegal activities. This paper corroborates the inclusion of end user and classification of activities prevalent on the nether side of dark net. Additionally, recounting the merits and demerits of browsing this web. The subject matter also demonstrates the association of this area of internet to cyber-crimes. Further illustrating the stipulation of the similar kind of happenings. The researcher tries to explains the impact of dark web activities on the existing society, covering the events that prevailed. The highlights in this article also gives a foresight into the future perspective of the upcoming trends associated with dark net. Further, the paper also reflects light on why there is a need for prevention of dark web activities covering the measures of practices for safety from the dark web.

Keywords: Dark web, dark net, cyber-crimes

Introduction

The Internet is broken down into three different regions: the surface, the deep, and the dark web. The dark web and the deep web, which are almost all of the Internet, are not visible to search engines. Due to various social and technological factors, the dark web has become a prominent source of illegal activities in the past few years. This paper aims to discuss the impact of this region on the Internet. Through the Internet, information is exchanged all around the world.

The dark web, which is a platform for anonymous communication, resides inside the global connection. According to the TOR Project, this type of anonymity can be achieved through the routing of traffic through multiple nodes. Anonymity can be abused by people to commit various cybercrimes, such as financial fraud, identity theft, and cyberextortion. A study conducted on the dark web revealed that it has become very popular since the launch of Silk Road, which was a drug marketplace that was shut down in 2013.Due to the increasing popularity of the dark web, it has been continuously monitored and analysed by law enforcers.

The dark web is different from the surface web in that it allows users to conduct unethical and ethical activities while maintaining their anonymity. It also has the capability to house a huge amount of harmful content. Authorities do not have a lot of control over the dark web. They only have limited steps they can take to monitor and analyse it. Some of these include mapping the directory of hidden services, keeping track of the social sites and customer data, and performing semantic analysis.

This paper aims to review the basics of the darknet and its role in the Internet. It also explores the ways in which it contributes to cybercrime and the efforts of law enforcers to combat illicit activities on the darknet.The paper's background segment explores the various aspects of the darknet. It then reviews the illegal activities and cybercrimes that are carried out on it. The third section provides an overview of the dark web's major roles. The paper concludes by examining the legal issues related to the dark web.

Background

The concepts of the dark web are often presented without context. This is because they are often misunderstood. Understanding the dark web requires a lot of research and practical experience.

The dark web is often the focus of headlines about illegal activities and breaches of data. These include the buying and selling of illicit drugs and pornography.The dark web is also used by people in developing countries to anonymously communicate with each other.During the 1990s, the concept of layered cryptography and networking was developed by researchers at the US Navy's NRL. The Tor browser is one of the most popular platforms used for browsing the dark web.

Understanding the dark web requires a lot of practical experience and research

This discussion aims to classify the web into three main categories.

1. The term "deep web" refers to websites that are inaccessible to users through major search engines such as Google and Yahoo. It is used by organizations and governments to store information that they need to protect. It is believed that the deep web is 500 times bigger than what the normal web is. Most of the content on this web is hidden away in a type of gate, and users need a password and username to access it.

2. The dark web is a collection of private networks or websites that are not indexable by search engines. It is used by various individuals and groups for anonymous and secure communication, as well as for illegal activities.

3. The surface web is open access to anyone using a browser and an Internet connection.

Online Anonymity of the dark web

Anonymity enables people to freely express themselves online as long as their offline self cannot be traced back. The rise of darknets and other similar technologies has made it easy for individuals with similar opinions to join groups where they can discuss their thoughts without boundaries.In platforms such as Tor, users can easily communicate with each other using pseudonyms or their chosen identities. However, Tor was able to separate the types of users on its platform in 2014.

A. **Civilians**: In Tor, people commonly use the anonymity of their online identities to protect themselves from identity theft and immoral markets. They also protect themselves from corporations that are irresponsible.While staying away from censorship, civilians prioritize research on sensitive subjects.

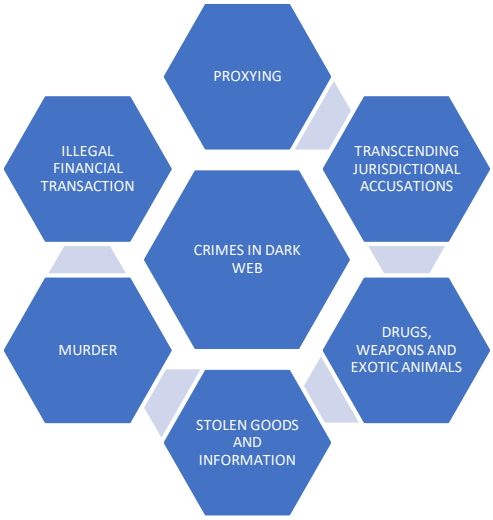
B. **Militaries:** In the past, military agents have been known to use Tor for their own purposes. They reportedly used it to gather intelligence.

C. **Journalists and their audience**: Due to the appeal of free speech, more journalists and people in developing countries have turned to Tor for their reporting needs. This allows them to keep track of local and regional issues and motivate political and social change.

D. **Law Enforocement**: Law enforcement agencies can also use Tor to monitor the activities of individuals online. This could include conducting sting operations, or maintaining anonymous tip lines.

E. **Activists and Whistle blowers** : Organizations and activists use Tor to report violations that could endanger their own lives. For instance, a whistle-blower can be taken away after revealing information that the company would rather keep secret. This is done through anonymous blogging and exposing corruption within the government.Anonymity is also considered a critical component of the dark web, as it allows users to keep track of their activities and prevent them from being exploited by illegal sellers. Despite the various policies that have been implemented to address the issue of online safety, the sociology of anonymity still needs to be studied.

Exploitation of the Dark web



1. **Proxying**: Due to the anonymity of the dark web, users are prone to getting proxy attacks. This is because the lack of a proper hypertext transfer protocol, which is known as https, makes it easy for a hacker to access a website. When a user visits a website, the hacker tricks them into believing that the site they are visiting is legitimate.A typical transaction involves using a non-traceable digital currency such as Bitcoin to scam the user. The hacker then transfers the money.The dark web chat Black Death regularly changes its URL. To ensure that the sites they visit are legitimate, users should mark them with a bookmark, which would allow them to verify the validity of the sites without falling victim to fraudsters or hackers.

2. **Transcending jurisdictional accusations**: The lack of physical barriers to the dark web prevents it from being traced back to a specific region of law enforcement. This eliminates the possibility of jurisdictional claims and convictions, which has been exploited by criminal organizations for a long time.

3. **Drugs, Weapons and Exotic Animals**: On the dark web, illegal websites like Silk Road operate similar to marketplaces such as eBay. They sell various items, such as clothes, books, unlicensed medicines, exotic animals, weapons, and illicit substances. The standard structure of these websites includes a short description, an image, and tiles for each item.Before Silk Road was shut down by the FBI in 2013, it was believed that illegal transactions involving various cryptocurrencies, such as Bitcoin, were conducted through the platform. The second version of Silk Road, which was known as Silk Road 2.0, was relaunched in a month. It took almost a year to find and shut down the site once it was re launched.In 2020, the website Agora was shut down. This caused AlphaBay to become the largest online drug marketplace. Other prominent dark web platforms that allow users to buy and sell illicit substances include Wall Street Market, Dream Market, and Valhalla. These sites mainly operate as illegal businesses.A report on the dark web claimed that the anonymity of the sellers caused a loss of reputation for the site.

4. **Stolen goods and Information**: Unlike the surface web, which is where software can be purchased directly, the dark web has separate websites that trade private information. These include the passwords, credit card information, and other personal details of users on various websites.Some of the most prominent websites that leak user information are PayPal, Creditcards for All, and Another Porn Exchange.

5. **Murder**: One of the most unethical activities that can be performed through the dark web is the execution of an individual. Due to the nature of the site, it is not possible to track the origin of the transaction. There are also marketplaces that allow people to make money from the murder. One of these is the Assassination Market, which allows users to bet on the death date of an individual.The information that the parties involved in the murder provide about the time of the killing gives them an advantage over the others. Even though the motive behind the murder is based on the profit generated by the betting process, the marketplace still gains due to its comparative nature.Since the bet is placed on the death date of the individual rather than the killing of them, it is very challenging to prove that the person who made the bet is criminally liable for the act. Some platforms, such as C'thuthlu and White Wolves, have complementary processes that allow users to hire assassins.

6. **Terrorism:** Terrorist groups need to develop an anonymous network to operate successfully. The dark web is a suitable platform for this purpose. It allows them to carry out their activities without being detected by the general Internet. This means that it is the ideal place to promote their activities.

7. **Exploit Markets** Prior to the release of a patch, a vulnerability can be introduced as a software flaw that's based on malware. A vulnerability that's not widely known to be exploited is known as a zero-day exploit. It can be found on recently released software that doesn't have a patch yet.Exploit markets allow users to perform transactions on these zero-day exploits. The prices of these exploit-based transactions vary depending on the popularity of the software and the difficulty in cracking it.

8. **Illegal financial Transactions**: One of the main illegal activities carried out by financial frauds on the dark web is the illegal use of financial instruments. Some of the prominent websites that allow users to perform such transactions are: InstaCard and Bankers & Co. These two websites allow users to conceal the source of their transactions and issue an anonymous debit card.Another illegal activity carried out through the dark web is the creation of virtual credit cards, which are issued by traders on the platform. According to Julia Dahl, there are numerous websites that allow users to purchase virtual credit cards, such as Atlantic Carding. Moreover, accounts of rich individuals can be bought and sold with the details of their users, as well as their names and addresses.The estimated loss caused by the Target data breach in 2014 was around 110 million dollars. Following this incident, numerous underground black markets flooded with stolen credit cards and account details.

9. **Arms Trafficking**: Another criminal activity that's commonly performed through the dark web involves the sale of weapons. One of the most prominent websites that sells weapons is Euroarms. It allows users to get their hands on various types of weapons. Besides guns, the website also sells ammunition.

10**. Child Pornography**: Due to the widespread disgust shown by the general public, the dark web has been known to allow users to access child pornography, which is incredibly hard to come across on a regular basis. The term "C.P." is often used to refer to this type of illicit material, which makes it easy to understand how prevalent it is on the platform.It's widely believed that the dark web allows paedophiles to access and engage in their activities through various forums and websites. According to a report by Tor, the highest traffic to its hidden sites came from child pornography. This has led to loathing for the individuals involved and the minors who are being used for such activities.In 2015, the FBI seized the website Lolita City, which had over 100,000 files, including videos and images with over 15 thousand users. The agency also took down another prominent website known as Playpen, which had over 200 000 users. The FBI was able to take down these two websites through a hacking tool that was used to identify the users of the websites.

Impact of dark web activities on the existing society

The dark web, also known as the Deep Web, has a reputation issue. Its mysterious nature makes it easy for people to speculate about what goes on in its various sections.

If you're living under a rock, then the dark web may be a subset of the internet that you're not privy to. It can only be accessed through search engines that can index its content. Compared to Google, it's slower. Most of the sites that are dark web are for legitimate purposes. They're there to protect people's anonymity online. Unfortunately, they can also be used to do things that are subversive and antisocial.

Dark web sites can be used to sell illegal drugs or weapons, which law enforcers often do not catch. In this article, we'll discuss the pros and cons associated with using the dark web.

Future perspective of the upcoming trends associated with dark net.

1. **Due to the nature of the dark web, it is expected to become even darker.**

Due to the challenging and inhospitable conditions that the dark web experiences, its operators constantly try to improve their services and make it more user-friendly. Due to their history of cause-based activities, extreme right-wing individuals are constantly looking for new ways to remain anonymous.

2. **The better the UX/UI, the lower the nerd factor.**

The user interface is often evaluated based on various factors such as the number of clicks to access, the load times, and the navigation schemes. The dark web's appeal has typically been attributed to being the lucky one who gets to find something hidden in the ocean of sludge. The dark web's evolution is expected to bring about a vastly improved level of search results.

3. **Darknet customer base will grow exponentially**

Due to the increasing number of articles and documentaries about the dark web, the consumer interest in it has greatly increased.In the past, people were hesitant to use the dark web due to rumors that those who use Tor would be placed on the FBI's watch list. With the abundance of Tor alternatives, as well as reports of "normal" individuals exploring the dark web for fun, more people are now open to accessing it

4. **The darknet will invent its own justice system**

There are no law enforcers, court systems, or lawyers available to address issues that occur on the dark web. This leaves a number of "fixer" sites to deal with the issues.Virtual world sites such as Second Life experienced a huge decline in user numbers due to issues that they could not resolve.Darknet justice is not a system approach to resolving disputes, but it could eventually evolve into a more practical method that everyone can adopt.

Why there is a need for prevention of dark web activities?

General Needs and Challenges

Rapid Changes in Volume of Use —Despite the existence of evidence of a steady increase in dark web activities, law enforcement officials still lack the necessary data to effectively address these activities.

Globalization: The dark web's cross-border nature makes it important that law enforcers work together to combat illicit activities. According to participants, if authorities fail to enforce the law on the dark web, it could encourage more criminals to conduct illicit activities.

The Need to Demystify the Dark Web: Some law enforcers noted that they are worried about exposing themselves to the negative effects of the dark web due to the lack of data on its activities. This issue is also reflected in the lack of transparency regarding the steps that law enforcers can take to address these issues.Participants noted that training programs for law enforcers should emphasize the similarities between traditional investigations and dark web investigations.

Technical needs and challenges

Despite the anonymity of the dark web, people can still use it to conduct illicit activities. According to a report by the RAND Corporation, basic tools such as a computer and internet literacy can help individuals start purchasing or supplying illicit goods online. The report also noted that law enforcement seizures can affect the entire market. However, users can still protect their information by using additional tools.

One of the biggest challenges law enforcers face when it comes to interdicting illicit goods through the postal systems is the volume of parcels that they have to deal with. The US Postal Service is estimated to move around 500 million parcels a day. In addition to having to deal with the large number of parcels, warrants are also required for most of the time when they seize illegal goods.During the workshop, the experts noted that they need to conduct studies on the gaps in the laws regarding searching packages.

Regulatory challenges

The anonymity and encryption of the dark web are some of the biggest obstacles that policymakers and law enforcers face when it comes to regulating the platform. This prevents them from gathering enough information to effectively combat cybercrimes.Due to the lack of a clear definition of what cyber terrorism is, it is now more difficult for intelligence agencies to determine its jurisdiction. The multiple threats that can arise from the internet are also linked to each other.

Dark web users can still conduct financial transactions in cryptocurrencies, which are known for their ability to provide anonymity. The blocks of cryptocurrencies are distributed across a network in a manner that's cryptographically secure.The way in which dark web users store and distribute information makes it incredibly difficult to modify or hack. For instance, the group responsible for the attack on the Colonial Pipeline demanded a huge sum of money in cryptocurrencies.

The REvil gang, which targeted hundreds of businesses in early 2021, also demanded a ransom in cryptocurrencies. Dark web users have been able to fund various illegal activities through Bitcoin transactions. Because of this, law enforcers have had a hard time tracking down the money trail, which is why it is only possible to regulate cryptocurrencies with regard to their legitimate use.One of the most important factors that law enforcers and policymakers need to consider when it comes to monitoring the activities of cryptocurrencies is the classification of all of their central and decentralized roles. This is because the blockchain technology that powers cryptocurrencies is still in its early stages of development. Another challenge that law enforcers face is the length of time that some dark web sites remain active.

Conclusion

The dark web is a place where individuals can perform illegal actions without leaving any evidence behind. All of the transactions and payments that happen on this platform are made using cryptocurrencies. Governments of various powerful nations use the dark web to carry out confidential activities. This is why it is important that the authorities take a balanced approach when it comes to addressing the issues related to this platform.Various private and public organizations can also help in addressing the technological issues related to the dark web by working together. This can help law enforcers develop effective tools and techniques to prevent criminal activities

One of the most important steps that can be taken to prevent data breaches is by implementing regulations that require companies to limit the amount of data they collect and automatically remove it from their systems after a certain period of time.Intelligence data collected from different organizations and sectors can be used to address the trans-border challenges of the dark web. This can be achieved through the establishment of international forums, seminars, and capacity building exercises.

End Notes:

➢ *The Dark Web and the Role of Secure Human Behaviors (isaca.org)*

➢ *The Dark Web and Regulatory Challenges | Manohar Parrikar Institute for Defence Studies and Analysesz (idsa.in)*

➢ *Greenberg, A; "How to Use Tor and Go Anonymous Online," Wired, 9 December 2017,www.wired.com/story/the-grand-tor/*

➢ *"How to: Use Tor for Android," Surveillance Self-Defense, 11 March 2020, ssd.eff.org/en/module/how-use-tor-android*

➢ *Sheils, C.; "Enter the Deep and Dark Web if You Dare (and Get Ready for a Surprise)," Digital.com, 5 August 2020*

➢ *Choudhury, S. R.; A. Kharpal; "The 'Deep Web' May Be 500 Times Bigger Than the Normal Web. Its Uses Go Well Beyond Buying Drugs," CNBC, 7 September 2018, www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-ofthe-dark-web.html*

➢ *Guccione, D.; "What Is the Dark Web? How To Access It and What You'll Find," CSO, 5 March 2020, https://www.csoonline.com/article/3249765/what-is-the-darkweb-how-to-access-it-and-what-youll- find.htm*