JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Research on Dark Web: Human Trafficking and Drugs

Gayatri Tawade[1] Engineering Student[1]
Amey Narvekar[2] Engineering Student[2]
Supriya Prajapati[3] Engineering Student[3]
Kartik Tandekar[4] Engineering Student[4]

Dr. Nilakshi Jain[5] Head Of Department[5]
Prof. Dipali Shende[6] Co-Guide[6]

Department of Cyber Security[1,2,3,4,5,6]
Shah & Anchor Kutchhi Eng. College, Mumbai, India[1,2,3,4,5,6]

Abstract : The internet offers anonymity through VPNs and onion routing. The Dark Web is a content that provides anonymity through technologies like traffic encryption, obfuscation, and forwarding. These mechanisms make it easy for cybercriminals to use illegal functionalities of the dark web and commit cybercrimes, which pose a threat to global security. Hackers now share information online about their cyber-attack plans, making the dark web accessible to a wider population. While this trend creates a vast amount of malware, it also provides intelligence for defenders to prepare for possible attacks. The combination of payment mechanisms, cryptocurrencies, and trust systems, together with the success of Tor's anonymity properties, has made marketplaces more attractive and resilient to hostile actions. However, law enforcement struggles with knowledge barriers and jurisdictional problems when apprehending perpetrators. This paper aims to analyze the mechanisms that the dark web uses to provide anonymity, its role in protecting criminals and allowing illegal marketplaces, and the different strategies that law enforcement has adopted to combat internet crime.

***IndexTerms* - dark web, drugs, tor.**

I. Introduction

The high level of confidentiality and limited traceability have made cybercrime on the Internet, particularly on the so-called dark networks, considerably more challenging to investigate. The tight protection of data travelling through the dark networks has rendered law enforcement with tedious and complex tasks that require extraordinary resources in terms of time, labour, knowledge, and competence. Users and administrators soon realized the privacy risks of the public Web and tried to protect content, user profiles, and communication with passwords and other authentication methods.

Dark web pages cannot be accessed with surface web browsers such as Chrome and Firefox because they typically adopt anonymous network technologies such as Tor, which encrypts the routing path between a client and a server to hide their IP address and the server name used during the connection. Tor also is the infrastructure that supports the Dark Web, i.e., the Deep Web content that exists on overlay networks, called darknets, that operate on top of the public Internet.

II. Guide to anonymous Dark Web

The Web and Data

To gain an understanding of the Deep Web, it is important to briefly review the origins of the Web. In the 1960s, the concept of a globally interconnected set of computers that could allow quick access to data and programs from any site led to the development of the Arpanet, which was a system of networked computers created to facilitate the sharing of resources, particularly for communication and information purposes. The Arpanet was a primary motivation for the development of the Internet as we know it today.

The Web's structure is based on three key protocols: the Uniform Resource Locator (URL), which provides a unique address for each page of information; Hypertext Transfer Protocol (HTTP), which is a computational language used to create distributed and collaborative information systems; and Hypertext Markup Language (HTML), which enables computers with different languages to translate information into a common language and communicate within a network. These innovations combined to create a space in which information could be communicated and travel around. While not all content on the Deep Web is illegal or illicit, caution should be exercised when accessing it, as there are potential security risks involved.

The Web's transformation since the 1990s has been largely driven by the centrality of data. As the number of web pages has continued to grow, an organizational system has become increasingly necessary. Examples of text retrieval web programs include Google and Bing, which use proprietary algorithms to check their databases for similar content to offer in return when a keyword is provided by the user. For example, when someone searches for a name on Google, its algorithms examine its databases and provide results that best match the searched topic in order of relevance. A search engine database requires two algorithmic processes: indexation, which involves selecting terms that best represent content, and matching, which involves comparing text representations between keywords and related data.

Online Anonymity

The significance of anonymous communications is apparent from various perspectives. Anonymous online interactions are now considered essential in safeguarding private information and reducing the risks associated with the Internet, such as hacking and malware. They also provide a means for people to engage in discussions on sensitive topics, such as health issues, through computer-mediated communication. Additionally, anonymous communications provide citizens with a means of avoiding government surveillance in both highly repressive and highly liberal contexts.

VPN services are a commonly used resource for granting anonymity, which can change a user's original IP address for another one in a different location, typically offering multiple geographical locations around the world to choose from. One primary advantage of VPN services for data protection from a privacy standpoint is that all the information shared by the user, regardless of the applications used, is immediately encrypted and dispatched through a secure tunnel established by the VPN server. However, due to the centralization of information by VPN companies, this service alone is not considered completely secure. The user's data may be used by the company for marketing purposes, or data about users may be released to authorities upon an official request. End-to-end encryption is another key tool for privacy, which works through a secret key shared by the sender and the receiver. This is a core technology for data security and data protection and constitutes a central component of the technical infrastructure of information society.

Contrary to ongoing discussions of online anonymity that characterize this issue as relevant to the actions and motivations of specific groups of users such as hackers, criminals, activists, or journalists, one should acknowledge that it characterizes to a certain extent any kind of online social interaction. Whenever users connect to the Internet, degrees of anonymity and non-anonymity are established that contribute to shaping their experience, its implications, and effects.

The Deep Web and the Dark Web

The World Wide Web, also known as the Web, is widely regarded as one of the most significant accomplishments of modern times. It has transformed the way we communicate and conduct business, presenting unparalleled opportunities. However, when the Web was originally designed, anonymity was not a primary consideration. Any user browsing the Web leaves behind digital footprints that can be traced back to their identity, making it easy to collect data to profile users. As a result, users and administrators quickly recognized the privacy risks associated with the public Web and implemented measures such as passwords and authentication methods to protect content, user profiles, and communication. This, along with paywalls restricting access to content and preventing indexing, resulted in the creation of the Deep Web.

The Dark Web has strong anonymity and freedom. The dark web can only be accessed with special software, special privilege escalation, or special settings on the computer. The Dark Web is located in the Deep Web, generally in the form of a private network (such as Tor or Freenet), or a peer-to-peer network (such as an I2P network). These types of networks rely on routing traffic on the network through the encryption layer to support users Anonymity. Supervisors cannot monitor routing information, nor can they obtain the true identity and location of both parties in the information exchange. Taking Tor as an example, after the Tor anonymous communication connection is successfully established, the double-sent messages of the communication will be encrypted, which can bypass the content review of the regulatory department, and can even complete illegal transactions, make extreme speeches, and even plan terrorist activities; and the onion routing of the Tor network mechanism makes the user's IP basically unable to complete the tracking, and the domain name of the onion website does not correspond to the exact addressable IP.

The Onion Router

The Onion Router (Tor) is a free and open-source software for anonymous communication networks. Tor uses a free, voluntary global coverage network consisting of more than 7,000 relay stations to redirect Internet traffic so as to conceal the user's location and usage from anyone conducting network monitoring or traffic analysis. Using Tor makes it more difficult to track users' Internet activities such as accessing websites, online posts, instant messages, and other forms of communication. Tor's intended use is to protect the privacy of its users and to protect its freedom and ability to conduct confidential communications by not monitoring its Internet activities.

Onion routing replaces TCP/IP networks that are used for general Internet browsing. TCP/IP networks break everything into smaller packets which all look for the best route to where they are sent. Implementing TCP/IP into a more anonymous format would involve using a mix network with it. Onion routing works by creating anonymous connections called circuits that work over a mix network. The onion routing system with the largest user base as previously stated is TOR (the onion router) which has "several thousand volunteer-operated nodes" or more commonly called tor relays. These relays process traffic globally from millions of users. The TOR anonymity network processes all "TCP based applications such as web browsing, email communication, secure shell, instant messaging, and chat services". A client chooses a path, and a circuit is made to complete that action. A circuit is made up of tor relays where each relay only knows the predecessor and the successor relays that make up the circuit. Traffic going through the circuit is "unwrapped by a symmetric key at each node" before being sent to the next node. It is called onion routing because each node unwraps another layer and onions have layers. Each relay also maintains a transport layer security or TLS-encrypted connection to every other relay in the network which helps the client build circuits through the network. The symmetric keys used at each relay hop is the reason nodes cannot trace connections they help form.

The basic steps of establishment of a connection between the local machine and the object in the Tor network are divided into three steps:

(1) Get the jump node: Before accessing the Tor network, the user installs the Onion Proxy (OP). The proxy sends a request to Tor's directory server. The directory server usually randomly selects several onion routes (usually an entry node, an intermediate

node) according to the strategy in the onion network. The Tor anonymous communication system is a link-based anonymous communication system, which is different from tunnel-based I2P. The jump node through which the data goes back and forth is the same, which means that once the user and the object determine the jump node for data transmission, these nodes are used for data transmission in a short period of time.

(2) Encrypted transmission. OP, ingress node, intermediate node, and egress node are adjacent to form a set of symmetric secret keys, which make the entire link multi-layered encryption. In this process, each relay node will only decrypt part of the content to obtain the next node The information is then transmitted, and only neighbouring nodes know each other's identity information, so that the anonymity of communication is realized. The steps shown in Figure 2.4.(a) are all encrypted and partially decrypted.

(3) Decryption arrives. All decryption is completed at the exit node, and the transmitted data will be transmitted to the object in plaintext. Survivability is a fundamental characteristic of largescale network, and would not disappear due to system evolution or external environment changes. In the largescale network, there exists information exchange between the failed subsystems and other subsystems, and thus may cause the cascaded failures. The increase of failed subsystems may cause the whole large-scale network failure (see Fig. 1).

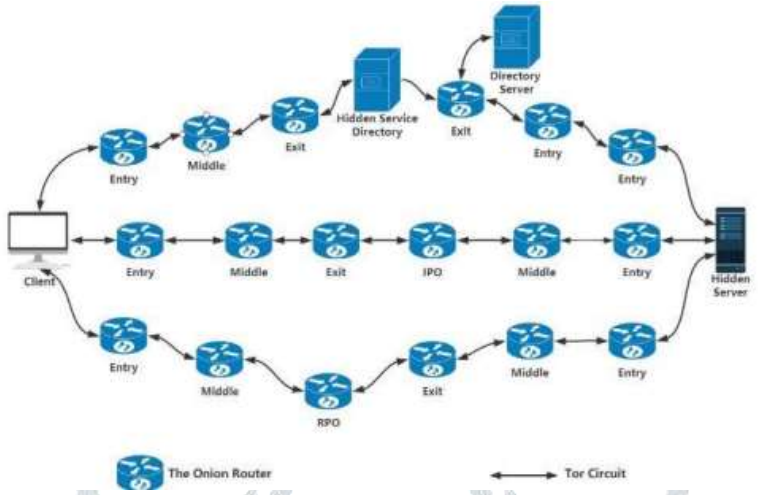


Fig.1 Tor Network Topology

III. Literature Review

The complexity of the dark web makes traditional detection methods to be effective. The research allows deep learning to be applied to the extraction to traffic features. [1]

This research analyses the current status of data collection research in the Dark Web, and analyses the applications such as threat intelligence collection perception, Underground Economy activity investigation with cryptocurrency tracking and tracing, Dark Web structural characteristics analysis, Dark Web and Surface Web Association analysis is introduced. [2]

It proposes countermeasures and suggestions to improve dark web information crawling from the three aspects of technology, personnel and upper structure. [3]

From the research findings it can be concluded that, the FBI has shown they are capable of fighting internet crime using online surveillance tactics and cyber-attacks to infiltrate illegal marketplaces. [4]

In this study, different feature selection approaches were utilized to determine best features, from Dark Web traffic data, that could help improve the prediction accuracy of malicious and benign activities. [5]

This paper aims to display the ability of DF software to track activity done on the Dark Web. The Dark Web provides criminals channels to perform illicit transactions, and as the Digital Age continues to evolve, more criminal activity will migrate into the cyber sphere. [6]

This analysis targeted the entire duration of these sites' activity, from 2013 to 2015. They focused on collecting ads and services related to malicious hacking and cyber criminality. [7]

This paper demonstrated how a reasoning framework based on the DeLP structured argumentation system can be leveraged to improve the performance of identifying at-risk systems based on hacker discussions on the D2web. [8]

Law enforcement agencies such as National Security Agency US conducting mass surveillance programs such as “Project Marina”, to trace down the cyber criminals and mass criminals worldwide. Most of the hidden networks such as “Playpen” (Child Pornography Site) mass sites have been seized by the FBI and CIA with using botnet malware running on dark web and revealing more than 20000 true IP Addresses. [9]

In this study, they proposed Standard Operating Procedures (SOPs) for Darkweb Forensics Investigation by considering the stage, objective of each stage, tools used in each stage and expected results. The proposed SOP consists of four stages, viz., identification and profiling, discovery, acquisition and preservation and the last stage is analysis and reporting. [10]

In this article, the documentation of these mechanisms, and investigate their role in the trading ecosystem. Systematically exploring marketplaces, vendor shops, and forums, provides insight on the factors that are contributing the most in shaping the state of the market. [11]

In this paper, we conducted an initial examination of malware products from 17 malicious hacker markets through unsupervised learning. Using manually-labeled data, we studied the effect of feature vector on cluster purity using text-based features. [12]

A fully automated open-source intelligence collecting tool has been developed, that crawls and extracts image-based intelligences from multiple onion based dark/deep websites. [13]

This work presents a temporal logic framework capable of predicting cyber-attacks in the near future. [14]

In this paper, the research helped in developing and applying a methodology to collect and analyze the content and involved Bitcoin addresses in Dark Web Shop websites. [15]

The research problem presented pointed out the need for data collection tools in dark web investigations and suggests a solution to the problem by presenting a prototype that fulfilled a number of requirements for such a dark web investigative software tool. [16]

These findings are relevant to law enforcement efforts in combating such offending behavior, as they provide the first description of this particular subset of individuals, many of whom will be entering correctional and rehabilitative services in the future, and coming onto the caseloads of forensic psychologists and other practitioners. [17]

The proposed approach develops an unsupervised model to monitor and characterize the Dark Web forums. [18]

This paper proposed a process for the e-commerce entity recognition task. [19]

In this study, we propose a multi-layer Bitcoin address clustering method using both blockchain-layer and application-layer information to resolve the false-negative problem associated with existing heuristics.

IV. Methodology

Problem Statement

In the Dark Web, criminals can operate illicit hidden marketplaces under the shelter of anonymity. Drugs, weapons, stolen credentials, exploitative content, and other illegal materials can be bought and sold in Dark Web markets. The Web provides criminals another avenue to operate in, and with the adoption of technology, more illicit activity will operate in Dark Web markets. Although tools like Computer Internet Protocol Address Verifier (CIPAV) can assist investigators in Dark web, there are no standard operating procedures for conducting an investigation. This is due to a lack of in-depth research regarding the Dark web investigation.

Need for research

The internet has helped to connect the world globally in a way many never thought possible. This increased globalization has led to user-to-user global marketplaces like eBay to grow in prominence. It has never been easier to find rare and unique goods online through these global services. However, the internet also is host to many more illicit marketplaces. Websites that deal in arms, drugs, trafficking, information (social security numbers and credit card numbers), and malicious malware. These websites are not as accessible as typing in the domain www.ebay.com, however, to those that know how to use VPNs (Virtual Private Network) and onion routing it is not difficult to find them.

Research Method

Onion websites are websites that use the .onion top-level domain and can only be accessed through the Tor network. Here are some methodologies for identifying dark web onion websites:

1. Use search engines designed for the dark web: There are search engines like Torch, not Evil, and Grams that are designed to search the dark web. These search engines index onion websites and allow users to search for specific topics or keywords.
2. Explore directories: There are also directories like the Hidden Wiki and OnionDir that list onion websites by category. These directories can be helpful in finding onion websites related to specific topics.
3. Use social media and forums: Some onion websites have social media profiles or forums where they promote their content or services. By following these profiles or participating in forums, users can learn about new onion websites.
4. Utilize word-of-mouth: Dark web onion websites are often shared through word-of-mouth. Talking to individuals who use the dark web and frequenting chat rooms can lead to new onion website discoveries.

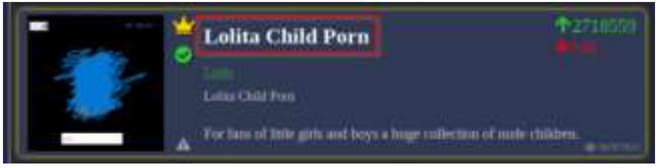
It is important to note that the dark web is a risky place, and accessing it can be dangerous. Users should take precautions such as using a VPN, using a secure operating system, and avoiding giving out personal information.

Major Research Findings

Ahmia is one of the search engines used on tor browser to find .onion links.

Fig.2 Ahmia (Tor links search engine)

Child pornography



Lolita Child Porn

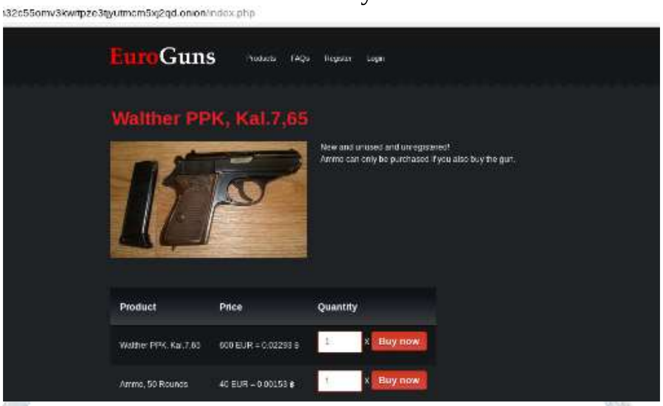
2718559

Lolita Child Porn

For fans of little girls and boys a huge collection of nude children.

Fig.3 Lolita (onion link)

Armory



.32c55omv3kwrtpze3tyutmcm5xj2qd.onion/index.php

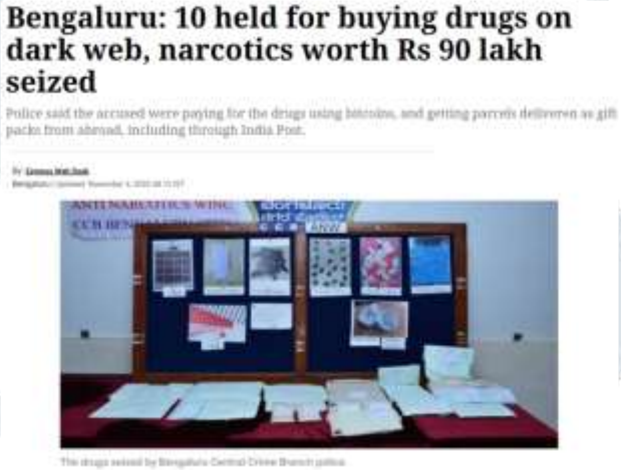
Walther PPK, Kal.7,65

New and unused and unregistered!
Ammo can only be purchased if you also buy the gun.

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 0.02293 ฿	1 x Buy now
Ammo, 50 Rounds	40 EUR = 0.00153 ฿	1 x Buy now

Fig.4 Euro Guns (onion link)

Recent news regarding Dark Web in India



Bengaluru: 10 held for buying drugs on dark web, narcotics worth Rs 90 lakh seized

Police said the accused were paying for the drugs using bitcoins, and getting parcels delivered as gift packs from abroad, including through India Post.

By [illegible]

ANTI NARCOTICS WING
CCB BEN

The drugs seized by Bengaluru Central Crime Branch police.

Fig. 5 Source: https://tinyurl.com/mvmw3pj9

Operation Blackface: New software will be cops' eyes, will track child porno suspects

By Abhishek Sharan / Updated: Dec 7, 2020, 08:07 IST

Fig. 6 Source: https://t.ly/mi72

Kerala Police to come up with 'Grapnel' tool to monitor darknet child porn sites

The Grapnel works by collecting data from websites, chat rooms and other sources.

Fig. 7 Source: https://tinyurl.com/4p43ff9a

Tech-Savvy Professionals Among 22 Arrested In Dark Web Narcotics Operation

The Narcotics Control Bureau (NCB) unearthed three major drug markets as it busted a pan-India drug trafficking network that used the dark web and cryptocurrency to courier narcotics at home.

India News | Press Trust of India | Updated: February 12, 2022 6:38 pm IST

Fig. 8 Source: https://tinyurl.com/2zzheepb

UP: Police arrest 4 in Lucknow for selling drugs through dark web in exchange for bitcoins

The Special Task Force of Uttar Pradesh Police arrested four men for supplying prohibited drugs in the international market through the dark web.

Fig. 9 Source: https://tinyurl.com/2b4bucaz

Lucknow: Gang procuring drugs from dark web for parties busted

TNN / Updated: Sep 8, 2022, 06:07 IST

Fig. 10 Source: https://tinyurl.com/mr2xj7ma

V. Conclusion And Future Scope

Dark web research is an essential area of study that has gained increasing attention in recent years due to its potential impacts on cybersecurity, law enforcement, and society. Through dark web research, we have gained insights into the various illegal activities that take place on the dark web, such as drug trafficking, human trafficking, cybercrime, and terrorism. Researchers have also investigated the role of anonymity, cryptography, and the Tor network in facilitating these illegal activities.

One of the significant challenges in dark web research is the difficulty in collecting and analyzing data due to the anonymous and decentralized nature of the dark web. However, with the development of new techniques and tools, researchers are making progress in overcoming these challenges.

The future of dark web research will likely focus on several areas. First, there is a need for more comprehensive studies to understand the scope and scale of illegal activities on the dark web. This can be achieved through the use of advanced data mining and analysis techniques that can uncover hidden patterns and relationships in dark web data. Secondly, as the use of the dark web continues to evolve, there will be a need to develop more advanced techniques for identifying and tracking criminal activities. This will require collaboration between researchers, law enforcement agencies, and cybersecurity experts. Thirdly, there is a need for more research into the social and psychological factors that contribute to the use of the dark web for criminal activities. Understanding the motivations and behaviors of dark web users can help in the development of effective strategies for preventing and combating cybercrime. Finally, with the increasing adoption of cryptocurrencies on the dark web, there is a need for more research into the links between the dark web and the wider cryptocurrency ecosystem. This includes understanding the impact of cryptocurrencies on the dark web economy and the potential for cryptocurrency-related crimes.

In conclusion, the future of dark web research is promising, and there are many opportunities for researchers to contribute to our understanding of this complex and ever-evolving ecosystem.

VI. Acknowledgment

We have great pleasure in presenting the project on “Research on Dark Web: Human Trafficking and Drugs”. We take this opportunity to express our sincere thanks to our Guide, Dr. Nilakshi Jain, Co-Guide Ms. Dipali Shende, the faculty in the Department of Cyber Security in Shah and Anchor Kutchhi Engineering College for guiding us and suggesting regarding the link of work. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would like to thank our Principal Dr. Bhavesh Patel and Dr. Nilakshi Jain, Head of Cyber Security Department, for their help, support & guidance for this project.

We are also thankful to all Faculty member of our department for their help and guidance during completion of our project.

References

[1] H. Ma, J. Cao, B. Mi, D. Huang, Y. Liu and Z. Zhang, "Dark web traffic detection method based on deep learning," 2021 IEEE 10th Data Driven Control and Learning Systems Conference (DDCLS), Suzhou, China, 2021, pp. 842-847, doi: 10.1109/DDCLS52934.2021.9455619.

[2] H. Zhang and F. Zou, "A Survey of the Dark Web and Dark Market Research," 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020, pp. 1694-1705, doi: 10.1109/ICCC51575.2020.9345271.

[3] Y. Xu, G. Chen, J. Wu, W. Xu and Q. Liu, "Research on Dark Web Monitoring Crawler Based on TOR," 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2021, pp. 197-202, doi: 10.1109/ICIBA52610.2021.9687954. -Research on Dark Web Monitoring Crawler Based on TOR

[4] R. Cole, S. Latif and M. M. Chowdhury, "Dark Web: A Facilitator of Crime," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 2021, pp. 1-6, doi: 10.1109/ICECCME52200.2021.9591011.

[5] A. Al-Omari, A. Allhusen, A. Wahbeh, M. Al-Ramahi and I. Alsmadi, "Dark Web Analytics: A Comparative Study of Feature Selection and Prediction Algorithms," 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA), San Antonio, TX, USA, 2022, pp. 170-175, doi: 10.1109/IDSTA55301.2022.9923042.

[6] R. Brinson, H. Wimmer and L. Chen, "Dark Web Forensics: An Investigation of Tracking Dark Web Activity with Digital Forensics," 2022 Interdisciplinary Research in Technology and Management (IRTM), Kolkata, India, 2022, pp. 1-8, doi: 10.1109/IRTM54583.2022.9791646.

[7] O. Cherqi, G. Mezzour, M. Ghogho and M. El Koutbi, "Analysis of Hacking Related Trade in the Darkweb," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 2018, pp. 79-84, doi: 10.1109/ISI.2018.8587311.

[8] E. Nunes, P. Shakarian and G. I. Simari, "At-risk system identification via analysis of discussions on the darkweb," 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, USA, 2018, pp. 1-12, doi: 10.1109/ECRIME.2018.8376211.

[9] K. Godawatte, M. Raza, M. Murtaza and A. Saeed, "Dark Web Along With The Dark Web Marketing And Surveillance," 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Gold Coast, QLD, Australia, 2019, pp. 483-485, doi: 10.1109/PDCAT46702.2019.00095.

[10] I.Paschal Mgembe, D. Ladislaus Msongaleli and N. K. Chaundhary, "Progressive Standard Operating Procedures for Darkweb Forensics Investigation," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-3, doi: 10.1109/ISDFS55398.2022.9800830.

[11] D. Georgoulias, J. M. Pedersen, M. Falch and E. Vasilomanolakis, "A qualitative mapping of Darkweb marketplaces," 2021 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 2021, pp. 1-15, doi: 10.1109/eCrime54498.2021.9738766.

[12] E. Marin, A. Diab and P. Shakarian, "Product offerings in malicious hacker markets," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 2016, pp. 187-189, doi: 10.1109/ISI.2016.7745465.

[13] A.Sasi, V. Nair and V. P, "DARKWEB IMAGE SCRAPPER: An Open Source Intelligence Tool," 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India, 2022, pp. 1-6, doi: 10.1109/CSI54720.2022.9924098.

[14] E. Marin, M. Almukaynizi and P. Shakarian, "Inductive and Deductive Reasoning to Assist in Cyber-Attack Prediction," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0262-0268, doi: 10.1109/CCWC47524.2020.9031154.

[15] K. Oosthoek, M. Van Staalduinen and G. Smaragdakis, "Quantifying Dark Web Shops' Illicit Revenue," in IEEE Access, vol. 11, pp. 4794-4808, 2023, doi: 10.1109/ACCESS.2023.3235409.

[16] J. Bergman and O. B. Popov, "Exploring Dark Web Crawlers: A systematic literature review of dark web crawlers and their implementation," in IEEE Access, doi: 10.1109/ACCESS.2023.3255165.

[17] Woodhams J, Kloess JA, Jose B, Hamilton-Giachritsis CE. Characteristics and Behaviors of Anonymous Users of Dark Web Platforms Suspected of Child Sexual Offenses. Front Psychol. 2021 Apr 9;12:623668. doi: 10.3389/fpsyg.2021.623668. PMID: 33897532; PMCID: PMC8062731.

[18] S. Nazah, S. Huda, J. H. Abawajy and M. M. Hassan, "An Unsupervised Model for Identifying and Characterizing Dark Web Forums," in IEEE Access, vol. 9, pp. 112871-112892, 2021, doi: 10.1109/ACCESS.2021.3103319.

[19] S. A. A. Shah, M. Ali Masood and A. Yasin, "Dark Web: E-Commerce Information Extraction Based on Name Entity Recognition Using Bidirectional-LSTM," in IEEE Access, vol. 10, pp. 99633-99645, 2022, doi: 10.1109/ACCESS.2022.3206539.

[20] M. Kim, J. Lee, H. Kwon and J. Hur, "Get off of Chain: Unveiling Dark Web Using Multilayer Bitcoin Address Clustering," in IEEE Access, vol. 10, pp. 70078-70091, 2022, doi: 10.1109/ACCESS.2022.3187210.

[21] J. Saleem, R. Islam and M. A. Kabir, "The Anonymity of the Dark Web: A Survey," in IEEE Access, vol. 10, pp. 33628-33660, 2022, doi: 10.1109/ACCESS.2022.3161547.

[22] N. Ferry, T. Hackenheimer, F. Herrmann and A. Tourette, "Methodology of dark web monitoring," 2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 2019, pp. 1-7, doi: 10.1109/ECAI46879.2019.9042072.

[23] De-Oliveira-Sarda, Thais (2020): The dark side of the internet: a study about representations of the deep web and the Tor network in the British press. Loughborough University. Thesis. https://doi.org/10.26174/thesis.lboro.12668612.v1