iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.58194

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

"Beyond the Shadows: Unraveling the Real-world Consequences of Dark Web Criminal Operations on Society"

Priyanka Ramakant Kadam
Ramnarain Ruia College, Software Engineer, Thane, India

Abstract: ***This study unveils the true consequences of criminal activities on the dark web within our society. The paper thoroughly analyzes the Dark Web and its profound impact. The Dark Web stands out as a highly challenging and untraceable medium embraced by cybercriminals, terrorists, and state-sponsored spies to pursue their illicit motives. Cybercrimes occurring within the Dark Web mirror real-world criminal activities.***
By exploring various dimensions of dark web criminal operations, this paper aims to offer a clearer understanding of their implications for society. Our goal is to unravel the intricate web of criminal activities and illuminate their impact on individuals, communities, and the overall well-being of society. Through a comprehensive analysis, we strive to enhance understanding and awareness of the complex relationship between Dark Web criminal operations and society at large.
Keywords: Dark Web, Criminal Activities, Internet, Cyber Criminals, Well-being of Society, Real-world Crimes.

I. INTRODUCTION

In this digital era, many are used to browsing through Google, which is www...where as he World Wide Web (WWW) is a complex system that consists of unprecedented amount of digital information. The normal Internet used daily is accessible through standard search engines such as Google and Yahoo. However, there are large sections of the Internet that is unindexed and hidden from the normal search engines. This widespread reliance on conventional search engines, however, but this habit often hides the secret side of the internet—the dark web [1]. The World Wide Web (www) consists of three parts i.e. Surface Web, Deep Web and Dark Web as shown in figure 1.

Figure 1. layers of internet

The Deep Web [2] is different from the surface web and isn't accessible to the general public. It's also known as the Invisible or Hidden web. About 96% of the internet falls into the deep and dark web category. It's mainly used for confidential purposes, like Netflix, online banking, webmail, dynamic pages, databases, and anything protected by passwords or paywalls. The Dark Web [3], although part of the World Wide Web, isn't accessible through regular browsers used for the surface web. Its origin traces back to the US Military, which employed it for discreet communication with remote intelligence assets. The dark web is infamous for hosting illegal activities and disturbing content, serving as a platform for terrorism, hacking, fraud services, phishing, scams, and even child pornography. It's essential to note that the Dark Web is a subset of the Deep Web. On the Dark Web, hidden services are prevalent, identified by onion extensions. For instance, Facebook operates a hidden service, and DuckDuckGo is another example. Specialized browsers, such as The Onion Router (TOR), FreeNet , Rife, Invisible Internet Project (I2P), and Whonix, are required to access the Dark Web.

According to the research it is difficult to truly measure the size and activity of the Dark Web, as many websites are under pressure from law enforcement, service providers, or their competitors. Despite this, several web intelligence services have attempted to map the reachable part of the Dark Web in recent studies. One crawled the home pages of more than 6,600 sites (before any possible login requirement), finding clusters of Bitcoin scams and bank card fraud [4]. Another study found that more than 87% of the sites measured did not link to other sites [5]. This is very different from the open Internet, both conceptually and in spirit: in contrast, we can view the Dark Web as a collection of individual sites or separated islands. Criminal activities and illegal contents are used with a percentage of 57% in the Dark Web. The associate editor coordinating the review of this manuscript and approving it for publication was Fabrizio Marozzo . There are lots of impacts of the Dark Web on Internet Governance. Besides criminal activities, illegal contents are also used on the Dark Web at a rate of 57%. Illegal drugs, fake currency child pornography, stolen financial details, weapon trafficking, illegal discussions, terrorist communication, and other crimes are common (Beshiri & Susuri, 2019). The challenge of unravelling illegal activities on the Dark Web is compounded by the formidable veil of secrecy provided by its services—a hurdle that forensic examiners confront with great difficulty (Chertaff, 2017; Alharbi et al., 2021). The utilization of unidentified services such as Tor, Freenet, I2P, and JonDonym is a common practice for accessing the contents and services within the Dark Web. As forensic examination becomes more critical in addressing illicit behaviors in this concealed digital realm, understanding and overcoming the intricacies of these covert services play a pivotal role in enhancing investigative capabilities. The clandestine nature of Dark Web activities necessitates advanced forensic methodologies and tools to decipher obscured trails and identify the perpetrators behind the illicit actions. The study of these anonymizing services becomes imperative for forensic examiners seeking to adapt and stay ahead in the ever-evolving landscape of cybercrime investigations.

In navigating the complexities of the digital era, we encounter various circumstances that shape our technological landscape. The study embarks the whole scenario to unravel the enigmatic realm of the dark web, exploring its clandestine activities and delving into the real-world consequences that extend far beyond the digital veil. That's why the title itself defines that this paper delves into the depths of the dark web, not merely as a technological phenomenon but as a complex ecosystem with far-reaching consequences for society. Beyond the Shadows: Unraveling the Real-world Consequences of Dark Web Criminal Operations on Society aims to explore the intricate interplay between the hidden recesses of the internet and the tangible impacts felt in our physical world. The allure of anonymity on the dark web has fostered a breeding ground for various illicit activities, from cybercrime and illicit trade to the dissemination of malicious ideologies. As we embark on this journey, it is imperative to recognize the dual nature of the dark web—a space that, while offering refuge to those seeking privacy and security, also harbors threats that extend well beyond the digital realm. Through a comprehensive analysis of the real-world repercussions of dark web criminal operations, this research endeavors to shed light on the often-overlooked consequences that permeate our society. In unraveling the layers of complexity surrounding this topic, we navigate the ethical considerations of balancing individual privacy with the collective security of society. By examining case studies, statistical analyses, and the narratives of those impacted, we aim to discern the true scope of the dark web's influence on our communities. For this purpose, we have systematically selected and reviewed 65 articles pertinent to our research aim. As we delve into the shadows of the Dark Web, the contributions of this paper are manifold. Firstly, it provides a comprehensive survey of the emerging crimes transpiring in the clandestine corners of the internet, unraveling the intricacies of illicit activities that often elude the public eye. Secondly, we meticulously explore the profound consequences of these crimes on social, economic, and ethical structures, shedding light on the tangible impact felt by society at large. It aim to enhance our understanding of the complexities surrounding the identification of these elusive individuals. Beyond the Shadows: Unraveling the Real-world Consequences of Dark Web Criminal Operations on Society*, these contributions serve as a crucial foundation for unraveling the hidden facets of the digital underworld and understanding the far-reaching implications on our interconnected world.

II. BACKGROUND

"In this section, the necessary background is introduced for understanding the concept of the real-world consequences of dark web criminal operations on society. Specifically, definitions and explanations of the underlying technological concepts related to the so-called Dark Web are provided."

A. The Deep Web and Dark Web

In the world of technology many are use to the internet from which we all can browse or access any kind of information we need. The media and academic literature frequently engage in discussions regarding two concepts: the Dark Web and the Deep Web. Due to the absence of precise official technical definitions, the utilization of these terms may lead to ambiguity. Consequently, these terms are frequently employed interchangeably and with varying degrees of exaggeration. Here, it's present the most widely accepted definitions, offering clarity to distinguish between both concepts.

1) The Deep Web

The term 'Deep Web' is employed in this study to characterize any form of online content that, for various deliberate or non-deliberate technical reasons, is not indexed by search engines. This stands in contrast to the 'Surface Web,' easily discoverable and accessible through common search engine providers. Deep Web content may be safeguarded by passwords, encrypted, disallowed from indexing by the owner, or not hyperlinked elsewhere. While certain content in the Deep Web may involve underground activities, such as accessible hacker forums without special anonymizing means, it also encompasses sites and servers serving legitimate purposes. This includes government web pages, traditional non-open academic papers, and databases, some of which owners may not even be aware are accessible over the Internet. Notably, private social media profiles on platforms like Facebook or Twitter fall within the classification of the Deep Web.

2) The Dark Web

In contrast, the Dark Web constitutes a segment of the Deep Web that is inaccessible through standard web browsers. Instead, specialized software is required, offering access to anonymity networks. Accessing the Dark Web demands intentional measures, ensuring strict anonymity for both users and service providers, as seen in underground forums. Various services facilitate practical access to anonymity networks, such as the Invisible Internet Project (IIP) or JonDonym [6]. Nevertheless, the most widely embraced manifestation of the Dark Web remains the so-called 'Hidden Services' offered by the Tor project. In the subsequent section, a comprehensive technical elucidation of Tor's Hidden Service feature is provided, serving as the foundation for the analysis conducted by BlackWidow.

B. Tor Hidden Services

Tor, originally an abbreviation for The Onion Router, is a project designed to facilitate low-latency anonymous communication by utilizing an encrypted network of relays. Users achieve anonymity by employing the principles of onion routing and telescoping, directing their communication through a Circuit comprising at least three relay nodes. As a crowdsourced network, Tor relies heavily on volunteers who operate these relays. The network plays a crucial role for various Internet users seeking anonymity, including dissidents and individuals in countries with restricted Internet access. Nevertheless, vulnerabilities leading to the potential deanonymization of Tor users have been extensively discussed in the literature. Given the decentralized nature of Tor, where the identity of every relay is not authenticated, concerns arise about the possibility of state actors, such as intelligence agencies, running their own relay nodes to exploit these vulnerabilities for deanonymization purposes [7]. Despite these potential threats, Tor remains the most well-known and widely used method for concealing one's identity on the Internet. In addition to providing users with the capability to connect to websites anonymously, Tor incorporates a feature known as Hidden Services. Introduced in 2004, this feature extends anonymity not only to the client but also to the server, a concept referred to as responder anonymity.

Specifically, when utilizing Hidden Services, the operator of any Internet service (such as a standard web page, including forums or message boards, pertinent to our investigation) can conceal their IP address from clients accessing the service. When a client connects to the Hidden Service, all data is directed through a designated Rendezvous Point, facilitating the connection of separate anonymous Tor circuits from both the client and the actual server [8]. Many of such services are known to such threats which can harm many of the features and access through the internet.

Figure 2 visually represents this concept, illustrating five primary components integral to a Hidden Service connection. These components include the Hidden Service itself, the client, the Rendezvous Point, an Introduction Point, and a Directory Server. This depiction offers a comprehensive view of the intricate network architecture involved in facilitating Hidden Service connections.

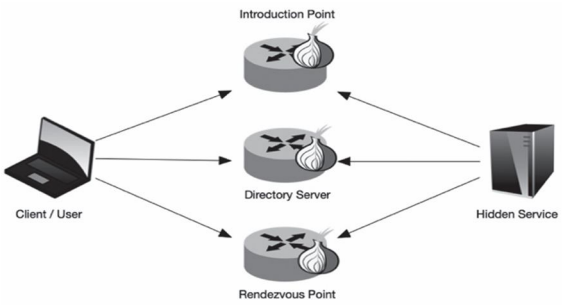


Figure 2. General illustration of the tor hidden service concept

The former refers to Tor relays responsible for forwarding management information necessary for establishing connections via the Rendezvous point. These relays are selected by the Hidden Service itself, a crucial step in connecting the client and the Hidden Service at the Rendezvous point. On the other hand, the latter pertains to Tor relay nodes where Hidden Services disseminate their information. This information is then communicated to clients, allowing them to learn the addresses of the Hidden Service's introduction points. These directories are typically published in static lists and are primarily used to discover addresses for web forums, a key aspect of the BlackWidow analysis. It is not surprising that Tor Hidden Services are an appealing concept for various underground websites, such as the notorious Silk Road or AlphaBay. Due to their widespread popularity, these services essentially constitute the foundational architecture of the Dark Web.

C. Historical Context

The concept of the dark web has its roots in the evolution of the internet and the desire for increased anonymity. Over the years, as technology advanced, the dark web became a platform for criminal enterprises to operate beyond the reach of traditional law enforcement. Understanding the historical development of the dark web is crucial for comprehending the challenges it poses to society.

D. Literature Review Scope

This article aims to review and present a comprehensive analysis of the anonymity of the dark web, featuring its key areas. Existing literature has extensively covered the technical aspects of the dark web and the various criminal activities that take place within its digital confines. However, there is a significant gap in understanding the tangible consequences of these activities on the broader society. Based on research there are some of the major objective areas which are collection of dark web data for Cyber Threat Intelligence (CTI) as the primary application domain. An integral aspect of our study involves an in-depth exploration of CAPTCHA as a significant challenge impeding the collection of data from the dark web , text-based CAPTCHAs. Specifically, it delves into image preprocessing techniques and background denoising methods, recognizing their essential roles in overcoming the challenges posed by dark web CAPTCHAs with intricate backgrounds. Identifying and organizing the most pertinent literature on the subject is a significant initial challenge for the literature review. The primary goal was to collect the literature and collectively give an overview of threats, their implementation, and the pattern of attacks followed by cybercriminals, which could help identify the baseline for researchers to design a prototype to mitigate such threats. This research aims to bridge this gap by exploring the social, economic, and psychological impacts of dark web criminal operations.

E. Rationale for the Study

The awareness of this study is needed for the well being of the society as cyber criminals ratios increasing day by day. While global law enforcement agencies have endeavored to counteract criminal activities on the dark web, there remains a restricted comprehension of the impact of these illicit endeavors on individuals, communities, and the broader societal framework. Conducting an exploration into the tangible consequences becomes imperative for enlightening policymakers, law enforcement personnel, and the general public regarding the gravity of the issue. It is essential for the development of effective strategies aimed at mitigating the adverse effects of dark web activities. Dark web is the wide web part of this scenario which are behind the shadows and there are many real world consequences of the same which is not in ratio number and may need a proper guidance to aware for well being of the society. All it depends on how you approach the internet is such way which can beneficial you.

F. Significance of the Study

This research is of paramount importance as it strives to unveil the concealed dimensions of criminal operations on the dark web and their ramifications for society.

A thorough comprehension of the impact enables us to proactively engage in the implementation of preventive measures, enhance cybersecurity protocols, and promote public awareness. These collective efforts are crucial in effectively mitigating the adverse consequences associated with dark web activities.

G. Research Objectives or Hypothese

Our objectives encompass the identification and analysis of distinct instances of criminal operations on the dark web and their linkages to real-world consequences. Furthermore, we aim to evaluate the social, economic, and psychological impacts on individuals and communities affected by these dark web activities.

In addition, our research seeks to delve into the challenges confronted by law enforcement in tackling dark web criminality and propose viable strategies for enhancement. This approach ensures the originality and authenticity of our research goals and contributes to the advancement of knowledge in this critical area.

H. Scope and Limitations

This study's scope is centered on particular case studies and instances illustrating criminal activities on the dark web, with a specific focus on their wider societal repercussions. However, limitations may arise due to the secretive nature of the dark web, posing challenges in acquiring exhaustive data on criminal operations. This acknowledgment emphasizes the originality and transparency of our research approach, recognizing the inherent difficulties associated with studying clandestine activities in this online domain.

I. Contextualize the Research Globally

While the dark web functions on a global scale, our research will contextualize its findings within the broader global context, recognizing the interconnected nature of dark web activities and their influence on societies worldwide. This articulation emphasizes the originality of our approach, acknowledging the global implications of dark web operations and their effects on societies globally. Dark web browsers are purpose-built web browsers crafted for accessing the dark web, an intentionally obscured part of the internet necessitating specific tools for entry. These browsers afford users the capability to navigate anonymously and reach websites featuring ".onion" domain extensions, exclusive to the dark web. Diverging from conventional web browsers such as Chrome, Firefox, or Safari, dark web browsers are intricately designed to augment privacy and anonymity.
Table 1. Summarize the dark web browsers in shortly.

Table 1. summary of browsers

Browser	Routing Protocol	Features	Anonymity Services	Disadvantages
Tor	Onion Routing	• Overlay Network • Free to access • Easy to install • Designed in C • Internet activity is not traceable through Tor • Provide anonymity to clients and servers • Tor supports all the Internet content • 3 Hop tunnels • Bi-directional tunnel • Bandwidth based peer selection	• HTTP • HTTPS • TCP • Remote DNS • Hides I.P.	• It does not protect against Traffic monitoring attacks • Not suitable for torrents, • Low Latency • It does not protect against Sybil attacks. • Can face high congestion leading to high latency due to circuit switching
I2P	Garlic Routing	• Easy to set up • Designed in Java • It provides an internal chat facility • Timing and man-in-middle attacks are difficult in I2P • Anonymous for torrents • File sharing is speedy • Best work with Linux • Distributed control system • Randomized number of Hops • Uni-directional tunnel • Performance-based peer selection	• HTTP • HTTPS • UDP/TCP • Remote DNS • Hides I.P.	• Not useful for windows and O.S. systems. • I2P does not guarantee anonymity for the surface web. • Documentation in different languages is not available in I2P • Memory usage is in efficient
FreeNet	Decentralized distributed data system	• It is peer-to-peer • Provide anonymity to the user requesting data and data carrier • Data can be transmitted over a	• HTTP • HTTPS • UDP • Hides I.P.	• Storage size is not fixed. • It does not protect again routing table insertion attacks.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

III. METHODOLOGY

The research entitled "Beyond the Shadows: Unraveling the Real-world Consequences of Dark Web Criminal Operations on Society" adopts a comprehensive methodology tailored to explore the intricate layers of dark web criminal activities and shed light on their tangible repercussions on individuals and society. This section furnishes a concise overview of the principal components and approaches that will guide the research process.

A. About Dark Web and Its Concepts

The Internet comprises three distinct levels: the surface web, the deep web, and the dark web as shown in figure 3. The surface web, the most familiar segment, is indexed by standard web browsers and widely accessible to the general public. In contrast, the deep and dark web constitutes unindexed portions of the Internet, beyond the reach of conventional search engines. This substantial portion of the Internet, accounting for approximately 96%, remains concealed.

As per the findings of Hayes, Cappa, and Cardon (2018), the dark web serves as a subset of the deep web, accessible solely through specialized tools like garlic, tunnel, or onion routing (such as Tor). This distinctive characteristic sets the dark web apart, ensuring a level of anonymity and restricted access beyond the capabilities of conventional browsing tools.

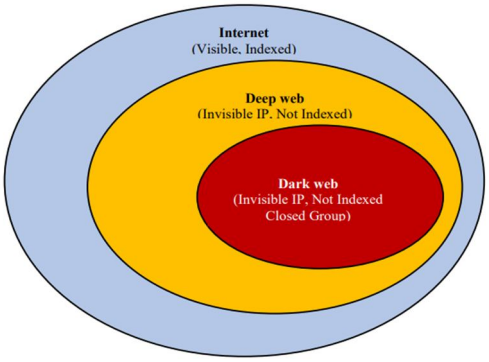


Figure 3.the surface , deep web and dark web

B. The Anonymity of the Dark Web

The following presents an overview of various techniques commonly employed to achieve anonymity and confidentiality on the dark web.

1) *Proxy:* Proxy services act as intermediaries between users and the Internet, functioning as gateways for filtering and bypassing. By serving as an intermediary server, proxies effectively separate end-users from websites, enhancing anonymity.
2) *Virtual Private Network (VPN):* A VPN establishes a private network, creating a concealed 'tunnel' from a device to the Internet. Encryption techniques are utilized to conceal crucial user data, offering an additional layer of privacy. Users often opt for paid VPN services like Nord or Phantom VPN, rendering internet activities untraceable [9].
3) *Domain Name System (DNS) Based Bypassing:* Regular browsers typically rely on DNS indices to access indexed websites, translating domain names into IP addresses. Dark websites, however, circumvent DNS-based indexing, preventing cross-pollination between the dark web and the regular web.
4) *Onion Routing:* Onion Routing is a pivotal feature in the dark web, providing anonymous connections through layered encryption during transmission. Messages are encrypted in multiple layers, resembling the layers of an onion, effectively concealing the identities of both the client and server [9].

C. Some Factors/Impact of the Dark Web are as Follows

1) Cyber Crime In The Dark Web

The landscape of criminal activity on the internet has evolved, rendering it more accessible to individuals seeking engagement in low-risk illicit endeavors. Simplicity characterizes activities such as orchestrating DDoS attacks on websites, where one can easily rent a botnet providing DDoS-as-a-Service (DDoSaaS). Additionally, deploying ransomware, capable of infecting unsuspecting individuals through phishing emails containing security-flawed links or attachments, has become a prevalent tactic (Tapor, 2019a). These services cater to malicious actors, particularly script kiddies, allowing them to target 'low-hanging fruit' – entities lacking sufficient security measures or training.

Moreover, dark nets inadvertently serve as recruitment platforms for budding hackers. As these individuals amass knowledge, they may eventually transition into roles such as law enforcement personnel or information security specialists, reflecting a shift where companies are increasingly considering the employment of individuals with hacking expertise (Tapor, 2019b). Tor's inherent confidentiality, and the difficulty associated with its deactivation, make it an ideal choice for Command and Control (C2) servers. Notably, botnet C2 services are among the conspicuous hidden services identified on the Tor browser. This convergence of technology and criminal activity underscores the evolving nature of cybercrime within the dark web.

2) Online Privacy in the Dark Web

TOR serves as a tool for enabling private, anonymous, and secure communications for specific purposes [10] [11]. The following examples illustrate its applications in the realms of anti-censorship, political activities, sensitive communications, and the secure transmission of leaked information:

a) *Anti-Censorship and Political Activities:* TOR is employed to circumvent censorship and access restricted destinations or content. It proves valuable in regions where certain information is blocked, allowing individuals to reach content that may be otherwise inaccessible. However, governments in some areas have implemented regulations or temporary blocks on TOR to counteract its usage. Notably, political dissidents in countries like Iran and Egypt utilize TOR to secure and maintain anonymous communications [10].

b) *Sensitive Communications*: TOR facilitates sensitive communications in chat rooms or forums for personal or business purposes. Its application extends to protecting children online by concealing their Internet browsing activities through hidden IP addresses. Businesses also utilize TOR to safeguard projects and counter industrial espionage efforts by competitors [10] [12] [13].

c) *Leaked Information*: Journalists leverage TOR for secure communication with informers and dissidents, ensuring the confidentiality of leaked information. Individuals can anonymously communicate and share documents with publishers through TOR, as exemplified by platforms like the New Yorker's Strongbox. Renowned whistleblower Edward Snowden utilized Tail, an operating system for anonymity that operates within TOR, to report and communicate with journalists, ultimately disclosing classified documents about U.S. defense programs. Snowden's revelations included a top-secret document detailing the NSA's attempts to de-anonymize users of the TOR browser [10].

3) Dark Web and Criminal Behavoir

The Deep Web and Dark Web are arenas where malicious activities are as prevalent as on the Surface Web. A spectrum of malevolent actors, ranging from thieves and terrorists to state-sponsored espionage, utilizes cyberspace. The internet serves as a platform for discussion, collaboration, and action, with the Dark Web providing enhanced capabilities for operations with reduced detection risks (Rafiuddin, Minhas & Dhubb, 2017). Although the focus in this discussion pertains to cybercriminals, the concerns raised are applicable to various harmful actors.In the twenty-first century, criminals increasingly leverage the internet and modern technologies for illicit activities. Traditional crimes like drug distribution and sex trafficking, as well as technologically oriented crimes such as identity theft, credit card fraud, and intellectual property theft, are facilitated through the digital realm. The Federal Bureau of Investigation (FBI) recognizes high-tech crimes among the most severe facing the United States.

The Dark Web is implicated in supporting a wide array of criminal activities, including the illegal sale of drugs, guns, exotic animals, stolen items, and data for profit. It hosts gambling sites, hired thieves, assassins, and repositories of child pornography. However, information scarcity persists regarding the prevalence of these Dark Web activities (Rafiuddin, Minhas & Dhubb, 2017; [14, 15]). Only approximately 1.5 percent of Tor users, according to Tor, browse secret services or Dark Web pages.

A University of Portsmouth study investigated Tor traffic to secret services by running 40 relay machines in the Tor network. The study provided unprecedented data on the total number of Tor hidden services online (approximately 45,000 at any given moment) and their traffic. While child abuse sites constituted around 2% of Tor hidden service domains, they accounted for 83% of all visitors to such sites, revealing a concentrated traffic pattern (Rafiuddin, Minhas & Dhubb, 2017). However, the results could be influenced by various factors.

A separate research effort by King's College London employed a web crawler to identify 5,205 active websites on the Tor network. Approximately half of these websites (2,723) contained material, with 1,547 classified as having illegal content. Notably, Tor estimated in 2015 that around 30,000 hidden services announce themselves to the Tor network daily, accounting for about 3.4 percent of overall Tor traffic. More recent statistics from March 2016 to March 2017 indicated an average of 50,000 to 60,000 daily hidden services or unique .onion addresses (Rafiuddin, Minhas & Dhubb, 2017; Yang et al., 2019).

The Dark Web serves various nefarious purposes, acting as a platform for organizing and coordinating crimes through chat rooms and communication services. Instances include tax-refund fraudsters sharing methods on the Dark Web (Yang et al., 2019). Additionally:

a) Malware used in large-scale data breaches to obtain unencrypted credit and debit card information is purchased on the Dark Web. For instance, RAM scrapers, a type of malware used in the 2013 Target hack, can be remotely deployed on point-of-sale systems.

b) Thieves monetize stolen data by selling it on the Dark Web. Following the Target data breach, underground markets were flooded with stolen credit and debit card account information, sold in batches for varying prices.

c) Data theft on the Dark Web is not only rapid but also prolific. In an experiment by security firm BitGlass, fabricated "stolen" data, including over 1,500 names, social security numbers, and credit card information, was uploaded to Dropbox and black market websites, accessing roughly 1,100 times in 22 countries within 12 days.

This comprehensive overview emphasizes the diverse criminal activities facilitated by the Dark Web, shedding light on its multifaceted role in enabling illicit operations.

4) CAM Investigation on the Dark Web

Investigating Child Abuse Material (CAM) is a challenging and tightly regulated activity, presenting difficulties for investigators due to its violent nature against children, leading to a stressful mental workload. The potential for suspects to build their defense during pre-trial and trial proceedings, utilizing hearings and information access, further complicates the investigative process. Ensuring the admissibility and weight of evidence becomes crucial, with uncertain evidence requiring careful consideration. Investigators dealing with Open-Source Intelligence (OSINT) material must exercise discretion, understanding the intelligence's context, creation timeline, and potential for alteration [16].

In CAM investigations, cross-border authority activities are pivotal. The material might be produced in one country, viewed from another, and involve victims and perpetrators from a third country, with investigating authorities potentially from a fourth. Effective information exchange and collaboration through organizations like Europol and Interpol play a crucial role in addressing this complexity.

The introduction of a CAM database in Finland and its integration with international cooperation mechanisms, such as Europol and Interpol, enhances the examination of CAM and facilitates collaboration. The private sector, particularly organizations like the Global Organization for Security and Intelligence (IOSI), can contribute significantly to CAM investigations. IOSI, acting as a consultant, laboratory, and incubator, focuses on shaping security and intelligence while promoting international security. Leveraging OSINT, IOSI aids law enforcement in identifying perpetrators and locating victims of child sexual abuse, connecting with OSINT experts worldwide. While IOSI OSINT experts may not process CAM directly, their knowledge can support and enhance the activities of law enforcement authorities.

CAM investigations may extend to the Dark Web, allowing investigators to examine sites containing CAM without personally accessing them. This approach enhances safety while maintaining the effectiveness of the investigation. This is how the U.S. Department of Homeland Security (DHS), among others, works.

The U.S. Department of Homeland Security employs methods to identify Dark Web users within the United States by monitoring file downloads through file-sharing services [17]. In a specific case, the DHS acquired the IP addresses of multiple suspects who accessed child pornography sites hosted on the Tor network. Researchers were able to trace all users who utilized the provided links to download an archive containing CAM from Dark Web. This investigation was undergone to know the consequences of such cases when it comes to criminal activities of Dark Web.

D. Attacks On The Dark Web

As previously mentioned, a multitude of cyberattacks originate within the dark web. The primary factor providing assurance to attackers is the anonymous feature inherent in the dark web. This section delves into various attacks on different browsers, with Tor being the most popular among them.

The categorization of these attacks is discussed in detail. Figure 4 provides a comprehensive overview of the attacks on the dark web discussed in this section.

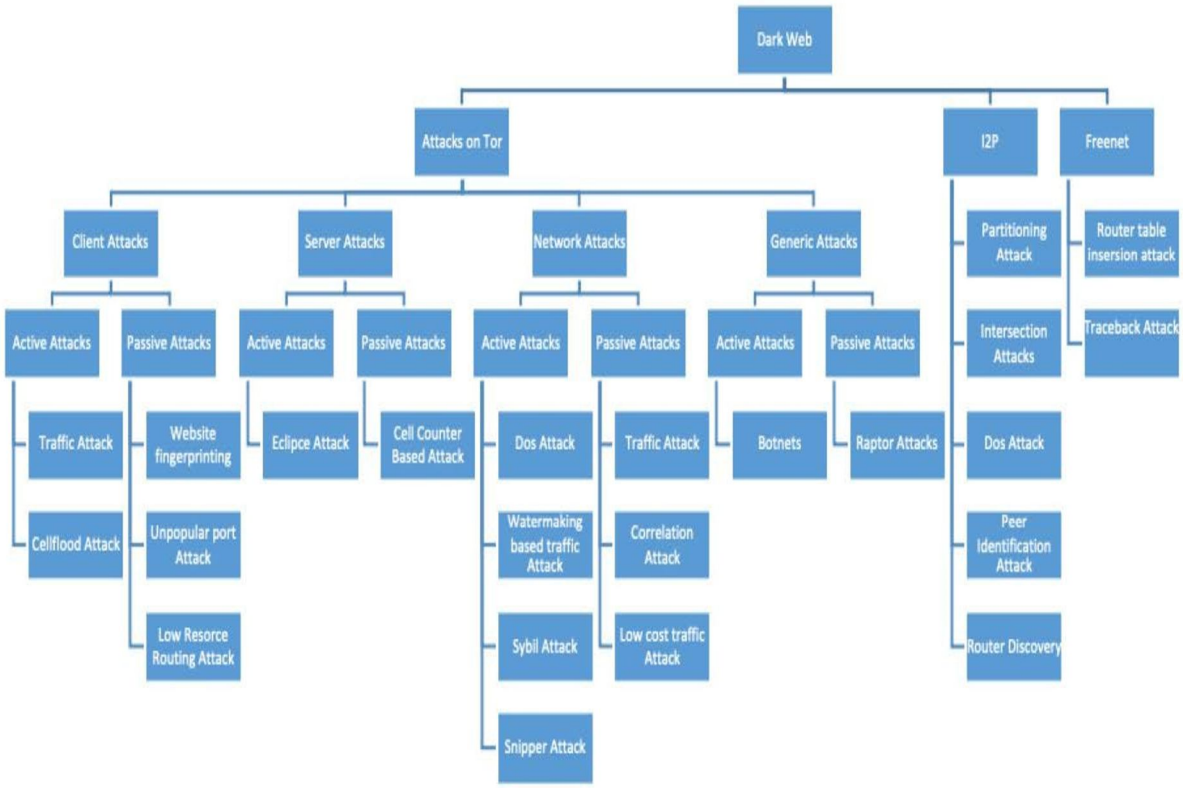


Figure 4. Attack taxonomy of the dark web

1) Attacks on Tor

While anonymity holds practical applications globally and is a fundamental necessity in the online realm, it, like everywhere else, faces intrusion from the cyber world's malicious actors engaged in various harmful activities. Tor, a widely used tool for achieving online anonymity, experiences multiple attacks each year, resulting in data breaches and the exposure of sensitive information. Verifier tools such as CIPAV (Computer and Internet Protocol Address Verifier) function similarly to malware, capable of collecting information despite the user's utilization of anonymizing technology. Law enforcement agencies employ these tools to track down cybercriminals and launch various attacks on secured anonymous networks, potentially causing significant harm. It is crucial for users of such technologies to understand these deanonymizing attacks, recognizing the limitations of the technology they rely on. Despite existing surveys on anonymous communication networks, a comprehensive survey addressing attack mechanisms on anonymity is currently lacking. Therefore, a comprehensive understanding includes two types of attack

i.Client Active Attacks and Client Passive Attack where as Client Active Attacks consist of Traffic Attack well these attacks vigorously insert a malicious program into unencrypted circulation at the server-side. Anonymity is compromised through the acquisition of control over a non-encrypted link, allowing the injection of various software instances such as Flash, JavaScript, ActiveX Controls, and Java. Once these codes successfully infiltrate any browser, they can circumvent the inherent security measures within the browser and establish a direct connection to the specific remote host. Through this process, the actual client's IP address can be exposed and obtained, breaching the intended anonymity[18]. Second, Cellflood Attack Barbara presented a practical and easy-to-perform cellflood attack [19]. This attack hampers Tor relays by flooding the circuit setup requests. Client Passive Attack consist of Website fingerprinting , Unpopular port attack and Low Resource Routing Attack , in this fingerprinting attacks are unique because they can be launched as active or passive. To reveal the clients' IP addresses, this attack can be transformed into an active one, involving the active manipulation of data at the application layer or the websites accessed by users [20].

2) Server Active Attacks

.Eclipse Attacks – These attacks afford attackers a cost-effective means to block random Tor hidden services. Researchers have implemented a significant prototype of the Eclipse attack to assess its impact on the live Tor network. They formalize the Eclipse attack process as a balls-into-bins problem, providing numerical estimates for the security of Tor hidden services [21].

Server Passive Attacks - This attack allows the invader to insert a signal at a cell counter of an entry or exit relay to influence the time of sending relay. On the other end of the circuit, the relay recognizes the rooted signal to confirm that a client communicates with a server.

3) Network Active Attacks

a) DOS Attack - Packet spinning introduces attacks using looping circuits and malicious onion routers, compromising anonymity. The looping strategy seeks to obstruct the selection of other onion routers. Two conventions govern this approach: circular circuits remain invisible, and a legitimate onion router will invest time in executing cryptographic calculations.

b) Watermarking Based Traffic Attack – In this threat scenario, the adversary inserts a signal or watermark into the target's traffic. Subsequently, the watermarked communication traffic is monitored to establish a relationship between the sender & receiver [20].

c) Sybil Attack – In June 2010, Tor relays experienced a sudden and substantial increase in a short period, indicative of a Sybil attack. It appeared that an entity had generated several hundred Tor relays on PlanetLab machines. While this might initially seem innocuous, it has the potential to be utilized for an attack on the Tor network, termed a Sybil attack. Figure 5 depicts datasets related to the assailant, agreement, and worker descriptors, as well as malicious transfers and the exit map [18].

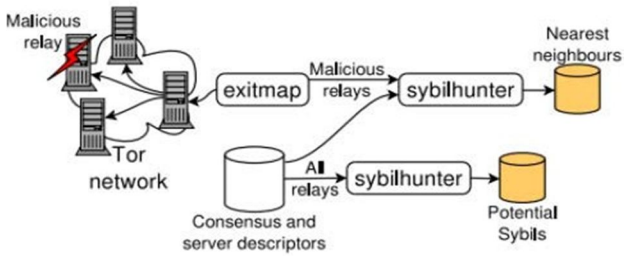


Figure 4. setup of sybil attack

d) Snipper Attack - Within a Tor circuit, traffic analysis is facilitated through an active watermarking technique that reveals the *communication* partners. The findings indicate that if a malicious actor targets the Tor network, the effectiveness approaches 100% with low latencies, making it challenging to detect.

E. Network Passive Attacks

a) Traffic Attack - The essence of an endways passive attack is to observe traffic without any active intervention and analyze the similarity between the sender's outbound and the receiver's inbound traffic. This technique can exploit packet counters, traffic pattern correlation, and timing correlation. For instance, the adversary monitors packets leaving and entering at both ends, and then applies a distance function based on traffic features to calculate the distance between these two links. The primary advantage of end-to-end attacks is the limited chance of detection since the traffic is only monitored. However, the true positive rate is low, while the false positive rate is high. As a result, an attacker can only discern traffic pattern similarities between senders and receivers over a significant amount of time. Additionally, end-to-end active attacks have been proposed to enhance the true positive rate and reduce the false positive rate by manipulating traffic to generate the desired signal [22].

b) Correlation Attacks – These attacks are crafted to identify communication relationships between clients and servers. These attacks, whether active or passive, operate as end-to-end attacks where the adversary observes both entry and exit nodes at both ends [20].

c) Low-Cost Traffic attacks - The term "low cost" in this context refers to a scenario involving a small-level adversary who possesses a limited view of the network, unlike global adversaries with visibility across all network links.

1) Generic Attacks

Generic Active Attack

Botnets – An overlay network is formed by compromising machines through the introduction of malware, creating a collective botnet controlled by an attacker. Bots within the network can be compromised through various methods, including 0-day exploits such as the notorious drive-by download technique [23]. In this method, users visiting a webpage may inadvertently download malware. Upon infecting the user's system, the botmaster gains the ability to command the botnet for illicit and malicious activities, including but not limited to Distributed Denial of Service (DDoS) attacks, spam campaigns, credential theft, cyberespionage, bitcoin mining, and more.

2) Generic Passive Attack

a) Raptor Attacks - Three distinct attacks leverage the Border Gateway Protocol (BGP) to orchestrate Raptor attacks [18]. Initially, attackers at the Autonomous System (AS) level infiltrate Internet routing to monitor at least one direction of user traffic. Due to the absence of encryption in TCP headers, packet numbers can be correlated at both ends, enabling malicious AS to inject these packets. Asymmetric traffic analysis simplifies the correlation of client and server by requiring only one direction of traffic at both ends of the circuit. In the second scenario, AS-level adversaries utilize Internet routing to manipulate BGP paths over time, inserting malicious AS nodes between the client and entry node with each change in the BGP path. These malicious nodes analyze traffic to ascertain the relationship between the client and server. As more malicious nodes are introduced over time, the likelihood of correlation also increases. The third tactic involves strategic adversaries using BGP hijacks to identify users of specific Tor guard nodes and analyze the traffic of these nodes.

3) Attacks on I2P

To overcome the centralized design limitations of Tor, researchers have suggested an alternative in the form of I2P, a distributed system. I2P stands out as the most intricate and promising anonymous Peer-to-Peer (P2P) system for several reasons.

a) Partioning Attacks - I2P sustains a distributed system by employing Kademlia and maintaining nodes in contact through NetDB. However, it's important to note that Kademlia is susceptible to partitioning attacks, which can isolate targets in the system and expose all parties engaged in a communication stream. A partitioning attack specifically targets end-users in the design, connecting to a smaller set of malicious nodes.

b) Intersection Attacks - These attacks entail observing a specific target and determining the number of nodes consistently linked to the system. The attacker leverages variations in tunnel rotation and target reachability to narrow down the nodes engaged in communication with the target. Consequently, the nodes involved in the target are closely monitored for any message traversal from source to destination. It's worth noting that these attacks can be combined with other strategies to enhance their overall effectiveness[24].

c) DOS Attacks - Cristopher Kack introduced a DoS attack against I2P, where malevolent I2P nodes repeatedly initiate numerous service connections in a cyclical fashion to deplete the resources of the targeted node [25]. In response, measures were taken to augment the availability of system resources in I2P. This included enhancements to total bandwidth, allowed tunnel limits, and memory size within the I2P router.

d) Peer Identification Attacks - Egger et al. [26] proposed a combination of attacks with a motive of peer identification using a particular service.

4) Attacks on FreeNet

As unrevealing the Sections, Freenet functions both as an opennet and darknet. This section delves into the attacks directed at the open mode of Freenet, accessible to anyone. Two specific attacks are scrutinized along with their corresponding countermeasures to provide insights into the anonymity framework of Freenet.

a) Routing Table Insertion Attack - The execution of a Real-Time Insertion (RTI) attack within Freenet involves three fundamental steps: gathering network topology and peer relationships, predicting routing paths, and inserting attack nodes into the target node's routing table. Freenet's code permits a node to autonomously choose its location, enabling RTI attacks to originate from any point in the network. When a new node joins, a controlled message broadcast is dispatched to other nodes, and based on bandwidth, multiple nodes may accept it as a neighbor. After responding to a predefined number of requests (typically 10), the new node replaces the least recently used peers. In an RTI attack, an assailant utilizes insertion and query nodes to insert keys into the intersection node, subsequently requesting these keys from the query node to inject the RTI attack into the targeted node. By manipulating the insertion and query nodes, the attacker can forecast the route to identify the intersection and target node [27].

b) Traceback Attack on FreeNet – Executing a traceback attack in Freenet involves two key elements. Initially, an attack node must establish a connection with a suspected node within the Freenet. This entails deploying numerous monitoring nodes throughout the network to detect content request messages. Upon acceptance of a pertinent content request message, the attacking node receives information in return, encompassing the content request message and neighboring nodes. This data aids in determining which among the neighboring nodes has encountered the corresponding UID [28].

F. The Impact of the Dark Web on Society

Discussions on the societal consequences of the dark web have sparked diverse viewpoints (Jardine, 2018; Kaur & Randhawa, 2020). Advocates argue that the dark web safeguards individual privacy, catering to citizens concerned about their privacy—a perceived positive outcome (Odendaal et al., 2019; Samtani et al., 2017). Conversely, critics contend that the privacy and anonymity offered by the dark web create opportunities for illicit activities, constituting a negative impact (Odendaal et al., 2019; Weimann, 2016). As Mador (2021, p. 6) notes, "much of the dark web is devoted to cybercrime," involving the sharing of techniques, tools, and the trade of stolen data and credentials. According to Kaur and Randhawa (2020), the dark web functions as a lucrative marketplace for criminals, generating substantial daily revenue, with activities ranging from hiring hackers to break into university systems for grade manipulation. This criminal reliance on the dark web has led to a surge in cybercrime, encompassing illegal drugs, stolen data, and password breaches, significantly impacting society negatively (Odendaal et al., 2019). Notably, the proliferation of malware on the dark web contributes to large-scale data breaches, aiming to acquire unencrypted financial information (Weimann, 2016). In essence, the societal effect of the dark web is a notable increase in cybercriminal activities. These cybercrimes encompass a wide array of illicit activities on the dark web, spanning drug trafficking, kidnapping/murder, human trafficking, firearms/weapons procurement, money laundering, contract hacking services, terrorism, and ransomware attacks (Table 2).

Table 2. mapping of reviewed papers on cybercrime activities conducted on the dark web

Cybercrimes	Study
Drug trafficking	Bertola (2020), Broséus et al. (2016), Me and Pesticcio (2018),Soska and Christin (2015), Aldridge and Decary-Hétu (2015), Duxbury and Haynie (2018)
Kidnapping/murder	Jin, Jang, Lee, Shin & Chung (2022), Lee et al. (2019), Melsky (2019), Taleby Ahvanooey et al. (2022), Zhou, Zhuge, Fan, Du& Lu (2020), Besenyő and Gulyas (2021)
Human trafficking	Burbano and Hernandez-Alvarez (2017), Taleby Ahvanooey etal. (2022), Kaur and Randhawa (2020)
Firearms/weapons procurement	Copeland, Wallin & Holt (2020), Taleby Ahvanooey et al. (2022), Revell (2017), Hayes et al. (2018)
Money laundering	Taleby Ahvanooey et al. (2022), Van Wegberg, Oerlemans and van Deventer (2018), Albrecht, Duffin, Hawkins & Rocha (2019), Bryans (2014), Volety, Saini, McGhin, Liu & Choo (2019)
Contract hacking services	Gupta et al. (2019), Taleby Ahvanooey et al. (2022), Odendaal et al. (2019), Samtani et al. (2017)
Terrorism	Chawki (2022), Chertoff and Simon (2015), Bates (2016), Nazah et al. (2020), Weimann (2016)
Ransomware attack	Chawki (2022), Ehrenfeld (2017), Gokhale and Olugbara (2020), Zhang and Chow (2020)

1) *Drug Trafficking* - The dark web has facilitated a transformative shift in the dynamics between drug vendors and buyers, introducing novel business models that capitalize on a different consumer base while mitigating risks associated with traditional offline markets, such as violence (Bertola, 2020; Broséus et al., 2016). The trade of illicit drugs dominates dark web markets, with a significant majority of activities being drug-related (Bertola, 2020; Me & Pesticcio, 2018). Approximately 57% of listings on dark web markets are estimated to involve drugs, marking a substantial presence in this clandestine online environment (Bertola, 2020; Soska & Christin, 2015). The crypto markets on the dark web have emerged as a distinct channel for drug trafficking, facilitating the movement of drugs across different regions through decentralized networks (Aldridge & Decary-Hétu, 2015; Bertola, 2020; Duxbury & Haynie, 2018).

2) *Kidnapping/Murder* - The dark web serves as a platform where individuals can engage in illicit activities related to kidnapping and murder by utilizing cryptocurrencies like Bitcoin for transactions (Jin et al., 2022; Melsky, 2019; Taleby Ahvanooey et al., 2022). Notably, certain dark websites facilitate real-world kidnapping schemes where cryptocurrency payments are accepted (Jin et al., 2022; Melsky, 2019). Additionally, the dark web provides a marketplace where individuals can hire hitmen for the purpose of orchestrating murders, with transactions often involving cryptocurrencies (Besenyő & Gulyas, 2021; Zhou et al., 2020). For example,in May 2016, a White-hat hacker named "bRpsd" reportedly helped the Federal Bureau of Investigation (FBI) to arrest some hitmen by hacking into the "Besa Mafia" site on the dark web and revealing contract information, which included client messages, user accounts, and other information. According to Taleby Ahvanooey et al. (2022, p. 4), "this concealed online platform facilitated connections between clients seeking hitmen services. The cost for a murder contract allegedly varied between $5,000 and $200,000". Moreover, individuals could also hire contractors for criminal activities like mugging instead of lethal actions (Lee et al., 2019).
3) Human Trafficking - The dark web serves as an anonymous marketplace for various illicit activities, including human trafficking and the procurement of illegal firearms and weapons. Traffickers engaged in human trafficking exploit encryption tools and frequently change between sites and profiles on the dark web to avoid law enforcement detection (Burbano & Hernandez-Alvarez, 2017; Taleby Ahvanooey et al., 2022; Kaur & Randhawa, 2020). In 2019, the US State Department reported a significant number of human trafficking victims, but the conviction rate for traffickers was comparatively low (Taleby Ahvanooey et al., 2022).
4) *Illegal Firearms/Weapons Procurement* - The dark web has also been misused for the illegal acquisition of firearms and weapons, with transactions often facilitated through the use of cryptocurrencies as a secure payment method (Taleby Ahvanooey et al., 2022; Copeland et al., 2020; Revell, 2017). This has raised concerns about the increased accessibility of weapons on the dark web, potentially contributing to criminal activities and acts of terrorism (Hayes et al., 2018; Taleby Ahvanooey et al., 2022). A study by RAND Europe in 2017 highlighted that dark web services have played a role in making weapons more accessible, comparable in price to the black market (Taleby Ahvanooey et al., 2022).
5) *Money Laundering* - Money laundering stands out as one of the prevalent criminal activities on the dark web (Taleby Ahvanooey et al., 2022). Criminals leverage the dark web to facilitate the transfer of illicit funds, such as the proceeds of crime, employing intricate sequences of transactions, often involving cryptocurrencies, to funnel funds into anonymous accounts (Albrecht et al., 2019; Taleby Ahvanooey et al., 2022). Bitcoin, a widely used virtual currency, is particularly favored for money laundering on the dark web due to its inherent anonymity, making it challenging to trace transactions (Van Wegberg et al., 2018; Bryans, 2014; Volety et al., 2019).
6) *Contract Hacking Services* - The dark web is teeming with hacking services, as numerous hacking forums and communities provide underground marketplaces for trading various tools, services, and stolen or leaked information (Taleby Ahvanooey et al., 2022; Gupta et al., 2019). Within these dark web spaces, individuals can explore different avenues to procure hacking services, making it an enticing environment for those seeking collaboration with members of prominent hacking communities (Odendaal et al., 2019; Samtani et al., 2017).
7) *Ransomware Attack* - Ransomware, a form of malicious software, involves the automatic encryption of every file on a computer's hard drive by the attacker, rendering them inaccessible to users. The attacker then demands ransom payment, usually in cryptocurrency, for the decryption of the files (Chawki, 2022; Ehrenfeld, 2017). An illustrative example is the Wannacry ransomware, notorious for automatically encrypting files upon download and causing substantial damage estimated at 4 billion dollars (Gokhale & Olugbara, 2020). Dark web websites typically utilize encryption, ensuring the confidentiality of user identities and maintaining the untraceable nature of activities conducted on these platforms (Zhang & Chow, 2020).

In summary, this section addresses the Real-world Consequences of Dark Web Criminal Operations On Society by delineating secven prominent cybercrime types prevalent on the dark web. It is evident that the dark web's untraceable functionality facilitates these cybercriminal activities.

According to Upulie and Prasanga (2021), cybercriminals leverage the dark web for discussions and illicit business transactions, taking advantage of the anonymity it provides. He, He & Li (2019, p. 73) emphasize that providers of illegal services use the dark web to publish illicit content, evading network law enforcement due to the difficulty in locating their real IPs, thereby exacerbating the abuse of the dark web. Importantly, these criminals may target vulnerable individuals or businesses without regard for national borders, seeking financial gains (Gupta et al., 2019).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

G. Law Enforcement in Criminal Investigations

Law enforcement grapples with a myriad of crimes, and initially, the surface web served as a platform for criminal activities. Websites like Craigslist and Backpage gained notoriety for crimes such as human trafficking, robbery, and murder. The proactive closure of Backpage by the U.S. Department of Justice stands as a significant example of law enforcement's active intervention.

On July 4, 2014, the TOR Project organization became aware of an attack on the subsystem of hidden services conducted by researchers from Carnegie Mellon. Subsequently, it was disclosed that these researchers were financially supported by the FBI. The TOR organization transparently shared comprehensive information about the attack, including technical details, on its blog. Users were advised to update their TOR software in response to the security concerns raised by the attack [29].

For law enforcement, TOR is a frequently utilized tool, primarily for three key activities:

1) *Online Surveillance:* TOR enables officials to browse websites and services of questionable nature without leaving any traces.
2) *Sting Operations:* TOR's anonymity features empower law enforcement officers to participate in undercover operations.
3) *Truly Anonymous Tip Lines:* Anonymous tip lines are widely popular, where information is submitted without attaching a name or email address. However, server logs can quickly identify the source of the tips.

H. Concluding the Unveiling the Actors of the Dark Web

The anonymity provided by the Dark Web can have both positive and negative implications. Online anonymity allows users to express opinions and impressions without constraints, as their online identities are not linked to the real world. To delve deeper into the various actors operating on the Dark Web and its activities, the Dark Web was accessed and crawled using the Tor browser and an Open Source Intelligence (OSINT) tool called TorBot. OSINT involves gathering information from openly published or publicly accessible sources [30]. Since the Dark Web is openly available to the public and accessible through specific software, developing OSINT tools to scrape information from Dark Web websites is feasible.

TorBot, the OSINT tool, was employed to crawl Dark Web websites, providing titles and short descriptions for each website crawled. The tool focused on scraping websites that function as main pages, offering directories of links to Dark Web websites. Two prominent websites, HiddenWiki and Torlinks, were crawled as they serve as URL lists for Tor hidden services. To explore the content of these websites, the Tor browser was used to access the Dark Web sites. Figure 5 showcases some results obtained through the TorBot crawling tool. It's essential to note that although the figure describes TorBot as an OSINT tool for the Deep Web, the Dark Web is part of the Deep Web.

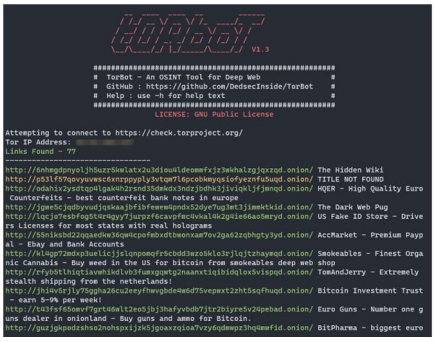


figure 5. torbot crawling's results on the hiddenwiki

I. Research Questions

The primary objective of this work is to summarize emerging crimes occurring in the Dark Web, outlining their consequences and defense techniques. Therefore, the research questions and motivations for this study are as follows –

1) What are the rising threats in the Dark Web crimes?

Recognizing the nature of Dark Web threats on a global scale is crucial in understanding how illegal content and services are accessed, and what their consequences are. This underscores the challenges involved and emphasizes the significance of developing improved technologies and enhancing law enforcement capabilities to track down criminals...

2) What types of techniques are applied to locate the criminals in Dark Web ?

Highlighting law enforcement techniques, current technologies, and emerging tools for tracing and detecting crimes in the Dark Web is crucial. This information paves the way for future strategies that involve leveraging the latest technologies in collaboration with law enforcement to thwart the plans of cyber-criminals...

3) How is the influence (%) of activities (the hidden services websites) in the Dark Web?

In a University of Portsmouth study, researchers collaborated with 40 relays (computers) operating on the TOR network and identified over 45,000 TOR hidden services websites. The findings revealed that 2% of these websites were associated with child abuse, and 83% of visitors had accessed these sites. Another study conducted by King's College London focused on TOR hidden services websites indexed by search engines like Ahmia and Onion City for the Dark Web. The research identified a total of 5,205 live websites, with 1,557 of them containing illicit content. According to estimates from the TOR project, hidden services' traffic accounted for approximately 3.4%. Between March 2016 and March 2017, an estimated 50,000 to 60,000 daily hidden services, each with unique onion addresses, were observed [31] [32].

4) What are the main types of criminal activities conducted on the Dark Web?

The Dark Web serves as a platform for diverse criminal activities, encompassing drug trafficking, kidnapping/murder-for-hire, human trafficking, illegal firearms/weapons procurement, money laundering, contract hacking services, terrorism, and ransomware attacks.

5) How does the anonymity provided by the Dark Web impact societal values and behaviors?

The anonymity provided by the Dark Web has dual effects, offering a space for unrestricted expression of opinions and ideas while concurrently fostering illegal activities. This duality results in an increase in cybercrime, encompassing drug trafficking, kidnapping, terrorism, and various other criminal pursuits.

6. How can the identification and understanding of Dark Web threats contribute to the development of technologies and policies that enhance cybersecurity?

By identifying and understanding Dark Web threats, the research aims to contribute to the development of technologies and policies that strengthen cybersecurity measures. This involves bridging gaps in current security frameworks and adopting proactive approaches to safeguard against evolving threats.

7. Can anonymity be verified in the Dark Web and can we say that it is the anonymous content?

The guarantee of complete anonymity on the Dark Web remains uncertain. While TOR aims to facilitate anonymous activities, ongoing efforts by researchers & security experts persist in developing tools to identify individuals or hidden services and potentially de-anonymize them.

Two illustrative examples that shed light on the intricacies of anonymity are as follows:1) In 2013, the Federal Bureau of Investigation (FBI) assumed control over Freedom Hosting. Several years earlier, the FBI had compromised the hosting service by injecting malware, specifically designed to expose the identities of visitors.

Since 2002, the FBI had employed a "computer and internet protocol address verifier" [10], functioning as malware within the Freedom Hosting service.

This malware enabled the identification and verification of suspects and their locations, even when they used proxy servers or anonymous services like TOR. 2) In 2017, members of the hacktivist group Anonymous reactivated and took control of Freedom Hosting II, the Dark Web hosting service and precursor to Freedom Hosting. Users associated with this content on Freedom Hosting could potentially be identified. Security experts estimated that Freedom Hosting II hosted between 1500 to 2000 hidden services, with around 15% to 20% classified as active sites [10].

6) What are the societal consequences of cybercrimes facilitated by the Dark Web?

The ramifications of cybercrimes on the Dark Web extend widely, contributing to drug addiction, violent offenses, human exploitation, illicit arms circulation, financial setbacks from ransomware attacks, and a general upsurge in criminal activities that adversely affect societal well-being.

IV. RESULTS

This section presents a detailed explanation of the dark web and its consequences. The dark web, a hidden realm beneath the surface of the internet, has long been a subject of intrigue and concern. In the research paper titled "Beyond the Shadows: Unraveling the Real-world Consequences of Dark Web Criminal Operations on Society," an in-depth exploration was conducted to understand the tangible impacts of criminal activities orchestrated within the shadows of this clandestine digital space. Leveraging case studies, including the notorious Silk Road marketplace, the study aimed to illuminate the profound consequences of dark web operations on individuals, communities, and the broader societal fabric.

A. A Case Study on The Silk Road

To exemplify the tangible effects of dark web activities, this study incorporates a detailed case study on The Silk Road. As one of the most infamous darknet marketplaces, The Silk Road played a pivotal role in shaping the narrative around hidden online criminal enterprises. By examining its rise, operation, and subsequent downfall, we aim to illustrate the concrete impact such platforms can have on individuals and communities[33].

1) Introduction

The Silk Road stands out as one of the most infamous darknet marketplaces, notorious for facilitating illicit transactions, including the sale of drugs, counterfeit currency, and hacking tools. This case study delves into the rise, operation, and eventual downfall of The Silk Road, shedding light on the legal actions taken against its founder, Ross Ulbricht.

2) Background

Launched in 2011, The Silk Road was a dark web marketplace operating on the Tor network, providing a platform for users to buy and sell goods and services anonymously using Bitcoin. Ross Ulbricht, operating under the pseudonym "Dread Pirate Roberts," founded the site with an initial focus on promoting privacy and libertarian ideals.

3) Rise of The Silk Road

The platform gained rapid popularity due to its decentralized structure, ensuring a level of anonymity for both buyers and sellers. The use of cryptocurrencies, particularly Bitcoin, further masked transactions. The Silk Road's success was attributed to its user-friendly interface, extensive product listings, and a secure escrow system that held funds until buyers confirmed receipt.

4) Illegal Activities on The Silk Road

The Silk Road became a hub for various illegal activities, primarily drug trafficking. Users could purchase narcotics, forged documents, hacking tools, and even hire hitmen through the platform. The site's pseudonymous transactions and escrow system provided a false sense of security for users engaging in criminal enterprises.

5) Downfall and Legal Actions

The illicit activities on The Silk Road drew the attention of law enforcement agencies worldwide. In 2013, the FBI successfully shut down the marketplace and arrested Ross Ulbricht in a dramatic operation. Ulbricht faced charges related to money laundering, computer hacking, and drug trafficking.

6) Trial and Conviction

During the trial, the prosecution presented evidence of Ulbricht's involvement in running The Silk Road. The defense argued that Ulbricht had created the platform but later handed it over to others. Despite the defense's claims, Ulbricht was convicted on multiple charges, including money laundering, computer hacking, and conspiracy to commit drug trafficking. In 2015, he received a life sentence without the possibility of parole.

7) Impact and Legacy

The case of The Silk Road had a profound impact on the dark web landscape. Law enforcement agencies increased efforts to combat illegal activities on darknet marketplaces, and subsequent platforms faced heightened scrutiny. The Silk Road's legacy serves as a cautionary tale about the risks and consequences associated with operating and participating in illicit online marketplaces.

The Silk Road, once a symbol of the dark web's potential for anonymity and freedom, ultimately faced a dramatic downfall. Ross Ulbricht's arrest and subsequent conviction highlighted the legal consequences individuals could face for facilitating criminal activities in the hidden corners of the internet.

B. Exploring Real-world Consequences

Our research navigates through the multifaceted impact of dark web activities on society. From drug addiction and violence to the exploitation of vulnerable individuals, the tentacles of these criminal operations extend far beyond the digital realm. As we unravel the layers of consequences, we aim to provide a comprehensive understanding of how the clandestine actions on the dark web reverberate in the real world.

C. Legal Responses and Societal Resilience

In addition to examining the repercussions, we scrutinize the legal responses initiated to counter dark web criminality. Case studies and legal actions, such as those against The Silk Road's founder, Ross Ulbricht, shed light on the measures taken to curb these activities. Furthermore, we explore societal resilience in the face of such threats, acknowledging the role of law enforcement, cybersecurity measures, and community initiatives.

D. Navigating Towards Solutions

As we unravel the intricate tapestry of consequences, our research also seeks to identify potential solutions and preventive measures. Understanding the dynamics of dark web criminal operations is a crucial step towards devising strategies that can mitigate their impact on society.

E. Conclusion

This research endeavors to move beyond the theoretical understanding of the Dark Web's criminal landscape, providing insights into the tangible effects on individuals and communities. By analyzing case studies and legal responses, we aim to contribute to a more nuanced comprehension of the challenges posed by dark web activities and foster discussions around effective countermeasures and societal resilience.

Figure 6. Timeline of the Silk Road

V. CONCLUSION

As discussed in this study , darkweb is a part of the Internet which is usually used by the users to do some activity in a hidden manner without leaving any traces. The research on "Beyond the Shadows: Unraveling the Real-world Consequences of Dark Web Criminal Operations on Society" delves into the intricate and multifaceted impact of dark web activities on various aspects of our society. The findings of this research shed light on the pervasive and often hidden consequences that extend beyond the digital realm, affecting individuals, communities, and institutions in profound ways. In response to these challenges, the study offers recommendations aimed at empowering law enforcement agencies, security entities, and IT security professionals to mitigate security threats emanating from the dark web, thereby safeguarding society. These recommendations are crucial in addressing the evolving landscape of cybercrime and ensuring a proactive approach to countering illicit activities conducted in the hidden recesses of the Internet. Furthermore, the study acknowledges its limitations, as it was confined to a systematic review. To enhance the understanding of the impact of the dark web, future research is encouraged to focus on collecting primary data. This approach would provide more nuanced insights into the dynamics of dark web activities and their real-world consequences.

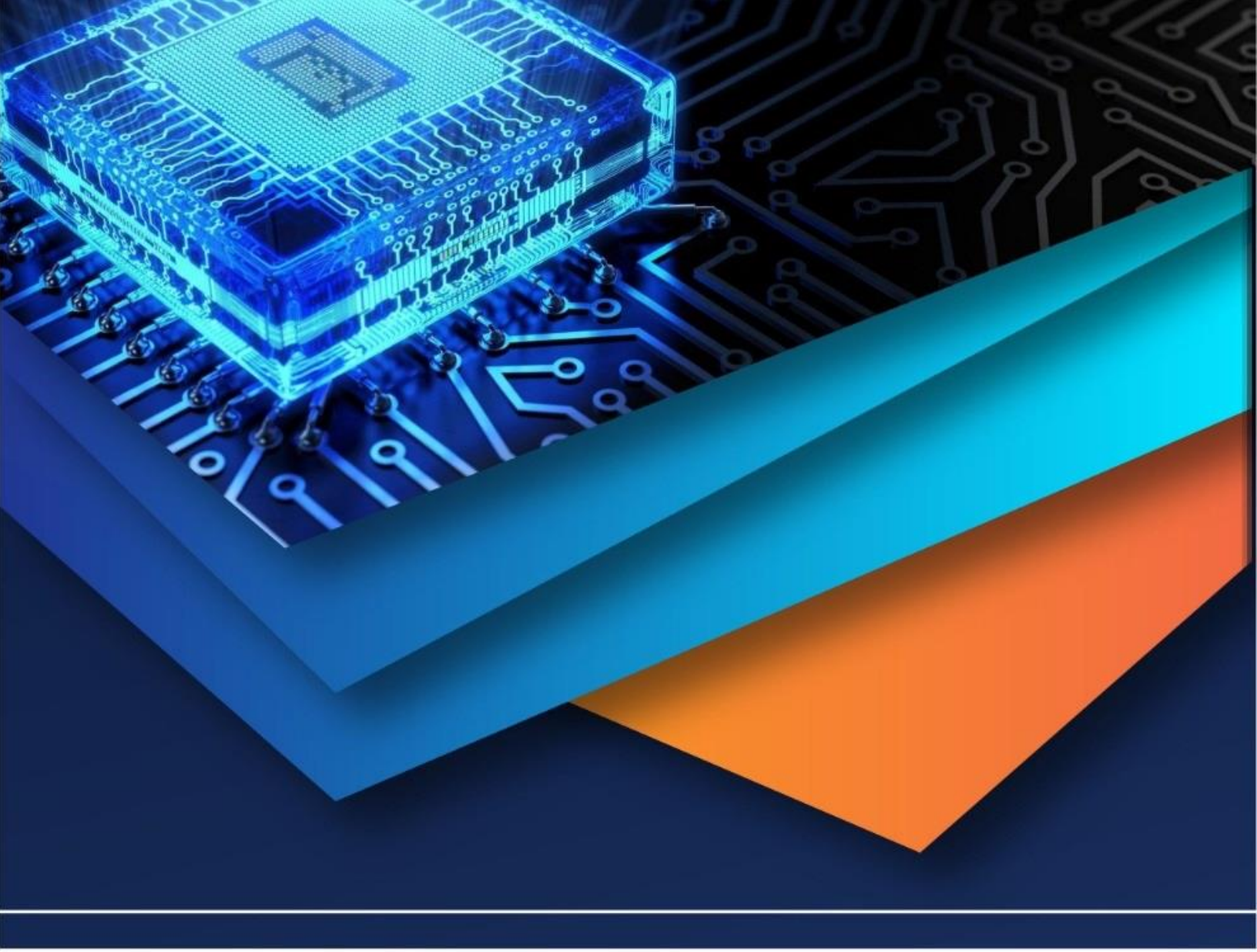
Additionally, the study suggests the need for future research to concentrate on awareness campaigns aimed at educating the public about the dangers associated with the dark web. Increasing awareness can contribute to a more informed and vigilant society, better equipped to recognize and respond to potential threats originating from the dark web.

Therefore, this study serves as an empirical foundation for future research endeavors in the realm of the dark web. By addressing the limitations and proposing avenues for further exploration, the study encourages a comprehensive understanding of the multifaceted challenges posed by the dark web and underscores the importance of ongoing efforts to protect individuals and society at large from its detrimental effects.

REFERENCES

[1] Stupples, ‘‘ICITST-2013: Keynote speaker 2: Security challenge of TOR and the deep Web,’’ presented at the 8th Int. Conf. Internet Technol. Secured Trans. (ICITST), Dec. 2013.
[2] Mirea, M., Wang, V., & Jung J. (2019). The not so dark side of the darknet: a qualitative study. Security Journal, 32, 102–118.
[3] Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the darknet: A qualitative study. Security Journal, 32, 102–118.
[4] Hyperion Gray, “Dark Web Map,” [Online]. Available: https://www.hyperiongray.com/dark-web-map/.[Accessed 7 1 2019].
[5] V. Griffith, Y. Xu and C. Ratti, “Graph Theoretic Properties of the Darkweb,” arXiv preprintarXiv:1704.07525, 2017.
[6] A. Pescape, A. Montieri, G. Aceto and D. Ciuonzo, “Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark (Web),” IEEE Transactions on Dependable and Secure Computing, 2018.
[7] K. Bauer, D. McCoy, D. Grunwald, T. Kohno and D. Sicker, “Low-resource routing attacks against Tor,” in Proceedings of the ACM Workshop on Privacy in Electronic Society, 2007.
[8] A. Biryukov, I. Pustogarov, F. Thill and R.-P. Weinmann, “Content and popularity analysis of Tor Hidden Services,” in IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW) , 2014.
[9] S. Saleh, J. Qadir, and M. U. Ilyas, ‘‘Shedding light on the dark corners of the internet: A survey of Tor research,’’ J. Netw. Comput. Appl., vol. 114,pp. 1–28, Jul. 2018, doi: 10.1016/j.jnca.2018.04.002.
[10] Finklea, K. (2017) Dark Web. Congressional Research Service, Washington DC, 10 March 2017, 1-19. https://fas.org/sgp/crs/misc/R44101.pdf
[11] Jardine, E. (2015) The Dark Web Dilemma: Tor, Anonymity and Online Policing. Centre for International Governance Innovation and Chatham House, 20, 1-24. https://www.cigionline.org/sites/default/files/no.21.pdf
[12] Yang, L., Liu, F., Kizza, J. and Ege, R. (2009) Discovering Topics from Dark Websites. Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security, Nashville, 1-5.
[13] Zhang, Y., Zeng, S., Huang, C.N., Fan, L., Yu, X., Dang, Y., Larson, C., Denning, D., Roberts, N. and Chen, H. (2010) Developing a Dark Web Collection and Infrastructure for Computational and Social Sciences. Proceedings of the IEEE International Conference on Intelligence and Security Informatics, Vancouver, 23-26 May 2010, 1-6.
[14] Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019, 28-31 May). BlackWidow: Monitoring the Dark Web for cyber security information. CyCon 2019: Tallinn, Estonia. https://doi.org/10.23919/CYCON.2019.8756845
[15] Topor, L. (2019a). Dark Hatred: Antisemitism on the Dark Web. Journal of Contemporary Antisemitism, 2, 2542. https://doi.org/10.26613/jca/2.2.31
[16] Fraser Sampson, ”Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings,” The Police Journal: Theory, Practice and Principles 90, no. 1 (2017): 55-69, https://doi.org/10.1177/0032258X16671031.
[17] “Child Sexual Abuse,” Global Organization for Security and Intelligence (IOSI), 2020, https://www.iosi.global/child-sexual-abuse/.
[18] B. Evers et al., ‘‘Thirteen years of Tor attacks,’’ 2016. [Online]. Available: https://github.com/Attacks-on-Tor/Attacks-on-Tor .
[19] M. V. Barbera, V. P. Kemerlis, V. Pappas, and A. D. Keromytis, ‘‘CellFlood: Attacking tor onion routers on the cheap,’’ in Computer Security— ESORICS (Lecture Notes in Computer Science), vol. 8134. Berlin, Ger- many: Springer, 2013, pp. 664–681, doi: 10.1007/978-3-642-40203-6_37.
[20] M. A. Sulaiman and S. Zhioua, ‘‘Attacking Tor through unpopular ports,’’ in Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst. Workshops, Jul. 2013,pp. 60–66, doi: 10.1109/ICDCSW.2013.29.
[21] Q. Tan, G. Yue, J. Shi, X. Wang, B. Fang, and Z. Tian, ‘‘Toward a comprehensive insight into the eclipse attacks of Tor hidden services,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 1584–1593, Apr. 2019, doi: 10.1109/JIOT.2018.2846624.
[22] P. Mayank and A. K. Singh, ‘‘Tor traffic identification,’’ in Proc. 7th Int. Conf. Commun. Syst. Netw. Technol. (CSNT), Nov. 2017, pp. 85–91, doi: 10.1109/CSNT.2017.8418516.
[23] M. Casenove and A. Miraglia, ‘‘Botnet over Tor: The illusion of hiding,’’ in Proc. 6th Int. Conf. Cyber Conflict (CyCon), Jun. 2014, pp. 273–282, doi: 10.1109/CYCON.2014.6916408.
[24] C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, ‘‘Practical attacks against the I2P network,’’ in Proc. 16th Int. Symp. Res. Attacks, Intru- sions Defenses (RAID), in Lecture Notes in Computer Science: Including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 8145, 2013, pp. 432–451, doi: 10.1007/978-3-642- 41284-4_22.
[25] M. Wilson and B. Bazli, ‘‘Forensic analysis of I2P activities,’’ in Proc. 22nd Int. Conf. Autom. Comput. (ICAC), Sep. 2016, pp. 529–534, doi: 10.1109/IConAC.2016.7604974.
[26] C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, ‘‘Practical attacks against the I2P network,’’ in Proc. 16th Int. Symp. Res. Attacks, Intru- sions Defenses (RAID), in Lecture Notes in Computer Science: Including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 8145, 2013, pp. 432–451, doi: 10.1007/978-3-642- 41284-4_22.
[27] T. Baumeister, Y. Dong, Z. Duan, and G. Tian, ‘‘A routing table insertion (RTI) attack on Freenet,’’ in Proc. Int. Conf. Cyber Secur., Dec. 2012,pp. 8–15, doi: 10.1109/CyberSecurity.2012.8.

[28] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, ‘‘A traceback attack on Freenet,’’ IEEE Trans. Dependable Secure Comput., vol. 14, no. 3,pp. 294–307, Jun. 2017, doi: 10.1109/TDSC.2015.2453983.
[29] “Confirmation Attack.” [Online]. Retrieved December 10, 2019, from https://blog.torproject.org/tor security-advisory-relay-early-traffi c-confirmation-attack.
[30] A. Sharma, John Breeden II, and Josh Fruhlinger, “15 top open-source intelligence tools,” https://www.csoonline.com/article/3445357/ what-is-osint-top-open-source-intelligence-tools.html, accessed 2023-06-20.
[31] Finklea, K. (2017) Dark Web. Congressional Research Service, Washington DC, 10 March 2017, 1-19. https://fas.org/sgp/crs/misc/R44101.pdf
[32] Ilou, C., Kalpakis, G., Tsikrika, T., Vrochidis, S. and Kompatsiaris, I. (2016) Hybrid Focused Crawling for Homemade Explosives Discovery on Surface and Dark Web. Proceedings of the 11th IEEE International Conference on Availability, Reliability and Security, Salzburg, Austria, 15 December 2016, 1-6.
[33] Armstrong, Q. (2021, September 24). A Timeline of The Dark web Market the Silk Road. Ranker. https://www.ranker.com/list/silk-road-dark-web-timeline/quinnarmstrong .



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY