International Journal of
Multidisciplinary Sciences and Arts

E-ISSN : 2962-1658
Volume 2, Number 2 , June , 2023
https://doi.org/10.47709/ijmdsa.vxix.xxxx

Dark Web and Cyber Scams: A Growing Threat to Online Safety

Nagaraju Arthan [1], Goutham Kacheru[2], Rohit Bajjuru [3]
[1]University of Cumber lands, Williamsburg, Kentucky.
[2]Infostretch Corporation, United States
[3]Southern Illinois University Edwardsville
[1] Narthan8486@Ucumberlands.edu, [2]Goutham.Kacheru@Infostretch.com, [3] rohitmyself17@gmail.com

open access

***Corresponding Author**
Natarajan Arthan
Narthan8486@Ucumberlands.edu

Article History:
Submitted: 06-06-2023
Accepted: 06-06-2023
Published: 09-06-2023

Key words
Internet, Dark Web, private investigations, unlawful activities, positive attributes, negative externalities, formal classification, access control, browsers, threats, attacks, exploits, malwares, types of offenses, Dark Web protection,

ABSTRACT

Internet as of now can be considered, and often is, a part of people's lives, a continuation of its existence; the same can be said about Dark Web: Indeed, when I first applied the analysis to the opportunity sample, with the blink of an eye, it can be readily deduced that this type belongs to the high opportunity type as well as the high threat type. Where in its so-called objectives of private investigations it has assigned the alibi for the mask of its authorizing it now becomes an opened invitation for unlawful activities. This papers therefore seeks to identify the dark Web and some of the positive attributes and some of the negative externalities that are inevitably associated with any attempted formal classification of access to and control over browsers. The following are threats that exist within the platform in the above said area described as attacks, exploits and malwares. They also categories type of kind's offence in the Dark Web in other to let more people know about existence of the areas and how to protect yourself.

INTRODUCTION

As we know the world is miles ahead with digitalization and technology, thus it has led to an increase in cyberspace; web security should be a major concern given that wherever you are, whatever time period each one of us happens to live amongst online now. What really changed is the rapid expansion of the Internet that made worldwide communication instantaneous and possible independent of where people were located, a major commercial breakthrough in the late 1990s. Yet such convenience exchanged anonymity for peace of mind: the underlying infrastructure of the internet was not built with privacy in mind, and early usages often required extensive identification that could be traced back to human activity. The absence of any privacy became a worry for different groups including the US Federal Government. It would take a coterie of computer geeks and mathematicians working at the Naval Research Laboratory, an arm of the US Navy, to begin developing its first incarnation in the mid1990s: Onion Routing. This technology intended to allow anonymous, two-way communication so that a third party could not tell where an online message originated or its destination. Onion Routing creates an overlay network a network that is built on subnet of the existing network, in this case, communication over the internet to provide anonymity. The overlay network (shown in Figure 1) is used to route data traffic, which conceals the source and destination of the traffic. Any networks that use onion routing are classed as Darkness.

The NRL understood that anonymity could not be expanded to true anonymity without broad availability, rather than just by the hand of the government. As such, they made their Onion Routing technology open source and The Onion Router started. This was a decision that opened up the doors of anonymous communication to the world and it laid an important foundation for what would come to be called the Dark Web. Such an evolution is a clear reflection of the fine balance between open transparency against privacy and security in the digital age.

Structure of the internet: There are three layers of the World Wide Web: Surface Web, Deep Web and Dark Web. The surface web accounts for only a small part (0.03%) of the internet and is accessible using regular search engines. The other part, which is believed to account for 96% of the internet is known as a Deep Web and not accessible by people. This includes Netflix, online banking, webmail, dynamic pages and databases that keep content behind passwords or paywalls. The Dark Web is a bit different it is not even accessible through standard browsing, but rather a smaller subset of the Deep Web. Originally devised by the US Military for secure messaging between remote intelligence assets, now a platform often linked to dark net activities. Example crimes: terrorism, hacking, fraud, phishing, scam & child porn

ORGANIZATION OF THE PAPER

Dark web is a topic that this paper covers several ways of it. The tools and protocols that underlie its development (e.g. browsers, encryption techniques, Virtual Private Networks and routing algorithms) is presented in Section 3.1 Emphasizes anonymity, includes your VPNs (like NordVPN and Phantom VPN) to use with these specialized browsers. Encryption is one of the critical techniques for Dark Web security. Connected to the Tor network, the Tor browser uses layers of encryption and random routing to hide the identity of users. But even on the Dark Web, centralized communication systems allow sensitive information to be shared at a risk. Solution: Pretty Good Privacy provides strong encryption for sensitive communication.

PGP uses asymmetric encryption using a public key and private key. A message encrypted with a recipient's public key can only be decrypted with the corresponding private key. PGP also allows verification through a blend of hashing and asymmetric cryptography. It fuses both a secret key and a public key encryption for the sake of privacy. As we can see (Figure 3) digital signatures consist of a secret key, hash function (one more time!) and two public private key pairs.

PGP has a lot of advantages: it protects one’s information from online theft, enables users to exchange data anonymously, refrains from recovering sensitive files once deleted, secures messages from getting infected, and one can check the registration of an alleged sender. Not enough information was provided about Dark Web technologies and anonymity, and to fully comprehend the issue, look into (Bernaschi et al., 2022) and (Nunes et al., 2016). A lot of browsers offer ways to access the Dark net, but each has some features. This narrative will illuminate the most extensive Tor network. In the 1990s, the United States Naval Research Laboratory began developing Tor. C, Python, and Rust are the languages in which it was written, and the alpha version was launched in 2002. Onion routing is used in Tor, where the user is encrypted and then passed through a series of intermediate nodes. The multiple pass scheme protects the data from researcher traffic and still provides location implementations of the client and the server. More circuit elements indicate more bandwidth, and the bound makes a user connection more difficult to track. Tor connections are globules composed of three types of relays, which are: 1. guard and middle relay. Thus, this two type forms the basic circuit of the Tor. Middle relays are therefore abstract list as a node passing traffic through it. 2. Exit relay. This relay is the final node in the circuit, sending traffic on to the destination, so that clients don’t reveal their IP to the server. Each relay only knows the predecessor and the next node on the circuit. 3. Bridge. Consequently, it hides the actual IP of the user, because the government or Internet Service Provider can knowledge the access that was depictured on the black list and block recognition in the public tor. Then the bridge has low hit risk and a bandwidth requirement. To learn about Tor and similar technologies,, , , would be read worthy. The Dark Web is built around anonymity and confidentiality. There are some techniques that keep these in check:

(i) Proxy: A proxy server is an intermediary functionality between the destination server and client. It then forwards requests from the client to a secondary server and sends back any responses from that server, hiding the user or client’s ip address. Proxy help bypass internet filtering and block to specific websites.

Tunneling/Virtual Private Networks: To provide a secure, encrypted connection (a "tunnel") over a public network such as the internet. It provides for private communications and the use of some resources, as if the user were directly connected to a private network. VPNs are usually for accessing a company intranet or getting around internet restrictions. They use Internet Protocol Security or Secure Sockets Layer protocols which make them more secure than proxies.

(iii) DNS Based Bypassing: Domain names (for example, google. It translates online domains (like www.example. It can also be used to bypass censorship.

Onion Routing: In contrast with the previous methods, the aim of onion routing is to anonymize the whole path in which a communication takes place. Information is encrypted in a multilayer (like an onion) and routed through numerous nodes. In this way not only the origin and destination, but also intermediate nodes can remain believe less, since each node decrypts a single layer to reveal the next node in the path.

Dark Web & Anonymity Related attacks

There are many approach vectors used against human users and services on the Dark Web, which maps to anonymity as well as security. These include:

DENIAL OF SERVICE ATTACK DISPERSED

DDoS attacks are those, in which the target server is flooded with fake requests, so that it uses up all of its resources and cannot be accessed by actual users. DDoS attacks do not operate towards directly deanonymizing users, rather they take down Dark Web services.

One such ambivalent incident is the Abraxas marketplace case. The disappearance of the exchange at the time of a Bitcoin price spike has often been attributed to an exit scam, though some evidence exists that a DDoS attack was involved.' It seems possible, given user reports of slow servers and inability to log in, as well as purported statements from Abraxas administrators on Reddit claiming a large DDoS attack. DDoS Prevention: Multivariate threat detection, can help efficiently catch and reduce DDoS attacks. Can you expose the sources that you are referencing along with and add them to your library? That would mean I could get at them and maybe be able to put some context on it.

Hidden Service Attacks

Attacks are also performed against hidden services, which are meant to be accessed anonymously. There are two main techniques that they use:

E-ISSN : 2962-1658
Volume 2, Number 2 , June , 2023
https://doi.org/10.47709/ijmdsa.vxix.xxxx

First Node Attack: An adversary tries to place their relay as the first Tor circuit node towards a hidden service. That then discloses the location of this hidden service. Malicious nodes and timing analysis is then used by attackers to find the first node.

Clock Skew Attack: This attack uses timestamps from different servers to identify the position of anonymous services.

PHISHING ATTACKS

Phishing is an attempt to gain sensitive information or install malware by deceiving users into believing they are communicating with a trusted source. This type of attack employs emails with hyperlinks or attachments that contain malware. There are three forms of phishing:

Spear phishing: It consists of personalized attacks on a specific organization designed to obtain sensitive information.

Whale Phishing: Aimed at high-level executives in companies, with highly customized messaging.

Clone Phishing: Deceives the target by providing a copy of an earlier email comprising of a legitimate message.

User Session & Websites Attack

In this part attacks directed towards user sessions and web sites are described with an emphasis on hijacking, man in middle attacks or cross site scripting.

Session Hijacking and Man in the Middle Attacks

Session management exploit is an activity in which an attacker hijacks your active session with a website or service. This is commonly done by somehow stealing the session ID, which are all private identifier. MITM attacks are a case where the attacker interjects and impersonates two parties to one another. As a result, the attacker will have the ability to listen in and even alter the data that is being passed.

These attacks are enabled by a number of techniques:

ARP Spoofing: The ARP stands for Address Resolution Protocol that matches IP addresses on a local network with the physical MAC addresses assigned to those devices. They hijack the ARP tables in such a way that traffic heading to a legitimate host goes into their machine instead.

Rogue Access Points: Attackers create fake WiFi access points that they say are legitimate ones; in doing so, the attackers encourage users to connect, which reveals their traffic.

mDNS Spoofing: Multicast DNS (mDNS) is used to resolve hostnames on local networks. mDNS queries can be replied to by attackers to redirect users onto malicious servers.

DNS Spoofing: DNS is what converts domain names to IP addresses. This method allows attackers to poison DNS caches so that when users try to navigate to a legitimate website, they are redirected elsewhere.

PREVENTIVE MEASURES

Robust Router Login Credentials: Default router login credentials and WiFi passwords must be altered to avoid unauthorized access.

Personal Virtual Network: VPNs provide an encrypted tunnel for internet traffic, protecting sensitive data.

Redirect all traffic to HTTPS: HTTPS secures the communication between browser and website.

Public Key Pair Based Authentication: Algorithms such as RSA authenticate the server to prevent users from communicating with unintended individuals.

Cross Site Scripting Attacks

Cross site scripting (XSS) is an attack on website users by injecting malicious scripts to vulnerable web pages. While SQL injection is an attack on the website's database, XSS exploits security vulnerabilities found in a website that allow it to accept untrusted content provided by users.

There are 3 main types of XSS attacks:

Reflected XSS: Attack scripts are embedded in the URL. As a user clicks such link, the script returns back and executes on their browser.

Persistent xss: Such type of malicious code is stored in the vulnerable server continuously, but it is mostly used for forums and comment sections. This script gets run every time the user opens the infected content.

DOM based XSS: When the client side scripts are compromised The attacker turns the browser's own Document Object Model to execute malicious content in that user's browser.

The outline should resemble this: Attacks Scalping Attacks Revised The old doc snippet (very rough) as was is something like; that doc snippet updated to revised version. Keep in mind, of course, if you had cited where you are getting this from, I could be more specific. You add sources to your library and cite them in your queries using the command.

Dark Web Malware Marketplace

As a natural consequence, the dark web is home to an exuberant marketplace for malware and services that enables illegal activity and lines the pockets of cybercriminals. Western Popularity For Malware Types In Dark Web Markets The Title Is “Dark Web Archives “Interactive: Focus Midia A report by Positive Technologies, based on research conducted during a single month in 2017 (with 25 dark web platforms tracked that had over 3 million users and 10,000 ads etc), provided data comparing malware types and previous estimates could range anywhere from just thousands to tens of thousands collectible clicks.

Popular Malware Types

Stealing Trojans – steal information such as passwords, keystrokes and files which can evade your Antivirus.

E-ISSN : 2962-1658
Volume 2, Number 2 , June , 2023
https://doi.org/10.47709/ijmdsa.vxix.xxxx

Ransom ware: This type of malware encrypts systems or files, then requests a payment to decrypt them. The average cost is $270. Organizations such as hospitals, government, law firms, and anyone protecting sensitive data have additional risk because they need to obtain information quickly and are even more susceptible to a security breach.

Remote Access Trojans: RATs allow an attacker to watch what a user is doing, take screenshots, execute commands, turn on webcams and microphones, and download files. DarkComet, CyberGate, ProRATBack Orifce bogger Cerberus RatSpyNetTurkojan are well-known RATs. They cost approximately $490, with some legitimate remote management software being repackaged for malicious usage costing approximately $1000 per month.

Botnet: Botnet Malware gives attackers the ability to take control of a network of infected devices. We offer packages from $200 to full services as $1000–$1500. Virobot is another example of botnet malware that combines ransom ware, key logging and spam distribution. Virobot allows users to encrypt data, steal the information they log in to the victim's device, and send spam mails from infected machines.

ATM Malware: These Trojans are focused on stealing cash from ATMs and charge a pretty penny, starting around $1500. Well, an ATM can hold large amounts (up to $200.000) of money thus this is a good target. This single malware instance can infect several ATMs

BEST PRACTICES TO ENSURE PROTECTION FROM MALWARE ATTACKS

The protection against malware is an approach with multiple angles: user education and training, great software hygiene, security reviews, backups, network security.

User Education:

Training: User training not to download and run unknown software

Identification: Help users learn to spot malware on their own (e.g., phishing emails)

Public Awareness: Regularly run security awareness campaigns.

Software Practices:

Trusted Antivirus/Antimalware: The first step in preventing malware on personal computers is to install and ensure that trusted antivirus and antimalware software is working, which detects, removes, and monitors these unwanted programs.

Website Security

Through Audits: Running the security scans within the website regularly to find and fix any loopholes is essential for both the organization and customer safety alike.

Data Backup

Backups: Maintain routine, reliable backups for data restoration following an attack or system failure.

Network Security: Intrusion Prevention/Detection Systems (IPS/IDS): Deploy IPS and IDS to monitor suspicious activity and block or alert on malicious network traffic.

Firewall: Use firewall to filter Ingress/Egress network Routes.

VPN: VPN should be enforced for remote access.

How the Dark Web Affects Cybersecurity and Internet Governance

The dark web is home to numerous crimes that affect cybersecurity both nationally and internationally. This part investigates the detrimental influences on cybersecurity and the challenges of internet governance & legal implications.

NEGATIVE IMPACTS ON CYBER SECURITY

There are a number of problems that illustrate the national security implications of the dark web:

Linked to Sensitive Info for Sale: Their research showed classified documents, such as those related to Unmanned Aerial Vehicles, were listed on dark net marketplaces. Data from breaches, such as the 2015 US Office of Personnel Management incident, is also commonly sold on dark web forums.

Illicit Familiarize with: Terrorist necessities are financed through dimnet courses. For instance, in 2018 Israeli law enforcement charged a man who tried to purchase weapons and transfer money to terrorists operating in Syria through the dark web.

Blowup of zero day exploits: Despite the vulnerability disclosure procedure, following ones are harmful. Those vulnerabilities are created for true malware (e.g., Stuxnet) but could also, later on, be repurposed and sold to foreign powers or criminals through the dark web and cause huge damage.

Legal Dimensions of Internet Governance: In recent years, the challenge for governments has been how to effectively regulate the dark web, when doing so often comes at the cost of loosening restrictions on anonymity and privacy violation in what may be innocent users. On the need for different government departments & agencies to work together, in order to translate research into effective policy. And while investigative law enforcement tools, like the FBI Computer and Internet Protocol Address Verifier to identify users hiding their relocation, do come into play.

Dark net Investigation and Governance

Law enforcement agencies use numerous methods to investigate dark web crime, and are continually searching for a middle ground when it comes to privacy. Some of these methods and the gaps demanding 층imited effective legal frameworks follows here.

Investigative Tools and Techniques:

Traffic Analysis: By breaking through anonymity services like Tor, authorities can color traffic patterns that help narrow investigations. We are helped in this by the fact that it is not hard to separate regular internet traffic from Tor traffic.

Memex: Memex, developed by DARPA, is a tool which helps expose trends in illegal activity without exposing all users instead focusing on the behavior of particular suspects.

Hacking: If users are visiting illegal sites on the dark web, the FBI has a method of figuring out who they are and their IP address – as happened in the Playpen case. It is also indicative of the need for legal frameworks to be in place to support such investigations.

The technical content of a CDS doesn't change for this issue, but creating and enforcing legal frameworks does.

Law enforcement works more effectively on the dark web than other platforms. This requires stronger legal frameworks both nationally and internationally to facilitate successful investigations. In this regard, perhaps no case better demonstrates the complications and legal nuance than Playpen, where the FBI was able to get a warrant to take over control of the server.

DARK WEB GOVERNANCE

There are a few areas that need to be monitored for effective governance of the dark web:

Hidden Service Mapping It is important to monitor and map the system used by Tor to hide its database a distributed hash table (DHT).

Monitoring Customer Data: Organization can identify possible threats by monitoring the requests for tracking of a toplevel domain name, which assists in mitigating the threat without violating the privacy rights of individuals. It emphasizes where the web requests ultimately go rather than what is in them.

Social Media Monitoring: Tracking wellknown social media channels can be useful for discovering hidden services and affiliate crimes.

PHOENIX: Conducting investigations on the dark web isn’t exactly the same as hunting down suspects in a small town. In this article, we discuss the involvement of law enforcement in dark web crime, why existing approaches are inadequate, and what changes might lie ahead.

Law Enforcement Activities

Under Online Surveillance — Using Tor for covert surveillance of ary suspicious site and services.

Sting Operations: Using Tor stealth for undercover operations

Anonymous Tip Lines: Similar to an online suggestion boxes, they seem anonymous; however, with good server logs, everything has a trace. Response to Carnegie Mellon/FBI Investigation of the Tor Project: Tension with Law Enforcement versus User Privacy

NOTABLE SHORTCOMINGS OF THE PRIOR METHODS

However these approaches are currently limited by a number of factors:

Scale of the Problem: The dark net is littered with potential new listings, all possessing a level of harm.

Ways they communicate: Sellers do not normally discuss buying malware on the regular internet, but exit to encrypted messaging applications (i.e., Telegram) – which makes tracking by law enforcement more complicated.

Malware Customization: Every malware is not a generic and is mostly tailored to buyer descriptions making it difficult for detection and prevention of those malwares.

Lure sophistication: Access to authentic materials—real company invoices and documents—peddled on the dark web enables criminals to produce extremely realistic phishing lures.

Future Directions

Both organizations and individuals can take several steps to reduce the risk posed by dark web activities:

For Organizations:

Comprehension of Threat: Establish Intelligence of dark web threats specifically tailored malware and remote access Trojans.

Intelligence collection: watch dark web markets for stolen data and malware aiming to, or prosecuted against the organization, in addition to brand attacks (e.g. cloned internet pages and billings).

Defensive Depth: Implement application isolation and threat telemetry for an additional layer of security to hinder any network intrusion

Anyway, the dark web can also be seen as a fruitful ground for competitive intelligence, recruitment or secure communications channels for criminals, so also difficult to navigate without ending up working with a criminal.

Use good browsing habits and stay on the lookout for phishing attempts, people. Please remember to keep their software up to date as well — all of it.

POSITIVE SIDE OF DARK WEB

The Dark Web: The Other Side of the Story

Dark web is always connected to illegal or clandestine ways, however, there is a lot more legit users that are using a dark web for their purpose. You might have not heard @Faisal3li when he said: The breakdown shows that most of its content is not criminal by a large margin: 54.5% to governments, tech companies, journalists, activists, etc.; 17.7% to defunct sites; only about onetenth (12.3%) to something we can broadly cite as "illicit drug trafficking activity," and less than a percent (1.3%) going to fraud/hacking‘ Such a wide range of content enables a microcosm of the dark web.

ADVANTAGES OF THE DARK WEB

Anonymity and Privacy: The dark web is very appealing to a lot of users because it provides you with greater anonymity. This draws in users who are worried about online privacy and surveillance by allowing them to surf the internet and communicate with others while shielding their identity and location. Even more so in countries with restrictive internet policies.

Reduced cost: In dark web marketplaces, certain items may be less costly than from regular sellers, or on the street markets (occasional bulk price breaks included).

Availability of scarce goods and services: The dark web often has access to commodities and services which are not easily available regional or via outside provider.

Convenient: Convenience of accessing and purchasing on these dark web marketplaces can be a big boon for some users.

Better Seller Reviews: Dark web forums tend to have a strong community of users sharing information on products and vendors, which creates transparency and accountability in the ecosystem.

Circumventing Censorship: The dark web can serve as a means to access information and communicate freely in countries with highly restricted internet access or strict censorship.

Niche Instruments and Offerings: The dark web has niche instruments like privacy email browsers, search engines with an eye toward discretion, etc.

LEGAL AND GOVERNMENTAL ACTIONS

Countries have taken different stances on the dark web:

● **USA:** A number of laws such as the Computer Fraud and Abuse Act make it illegal to access a computer without proper authorization, alter or cause damage to those systems, or traffic in passwords and other devices for accessing computers.

● **Russia:** It is a political motivation for DE anonymize Tor users.

● **China**: The communist government makes active efforts to prevent access to the Tor network.

We need to keep in mind the dark web is as complex an environment as any, and it has advantages along with disadvantages. The dark web has its pros and cons that give us both a comfort of privacy to rely upon as well as the dangers our freedom bring in front of illegal acts taking place on it. Grasping these complexities is key to figuring out how to intentionally explore and navigate this hidden region of the internet.

6 Facts about the Dark Web; an Interesting Overview

DARK WEB: FACTS AND FIGURES

The dark web which is seen by many as a hotbed for criminal activity generates significant revenue with estimates of over $500,000 every day. Gray whales are also known for their size, which in 2001 a University of California study estimated to reach 7.5 petabytes wide with both legal and illegal activities occurring at the same time.

Usage & Criminal Acts

● Use of Crypto currency in Payments as Bit coin, a crypto currency, cannot be decrypted due to their anonymity and expensive transaction traceability; it is also commonly used for payments.

● Terrorists have exploited the dark web for purposes of propaganda, recruitment and fundraising such as ISIS.

● **tracking and DE anonymizing:** As we know, spy agencies such as the NSA use tools like X Key score to find out who is using Tor.

● **Fake documents:** According to Israeli intelligence firm Six gill, fake diplomas, certificates and passports are all for sale.

● **Academic Fraud:** Hackersforhire are available to breach university systems and change grades.

Scams and Fraud the dark web is a hotbed of scams, making for an environment where you truly need to protect yourself.

Child Pornography: As per estimates around 80% of dark web traffic is linked to child pornography, which is yet another extremely disturbing statistics.

● Website Hacking — on average 30,000 websites are hacked every day.

● Match Fixing & Unlawful Wagering — the dark web is used to grossly matchfix and unlawful wagering and so on.

BEYOND ILLICIT ACTIVITIES

So, while the dark web is often seen as a hotbed of criminality, it does contain some perfectly legitimate communities and resources:

Book clubs & lit: Clubs and bazaars for access to conspiracy theories, banned literature, and other niche publications

Survivors Information: Strategic Intelligence Network and others offering information about crisis management and survival techniques

Scale and Scope:

With an estimated 550 billion single documents residing within the dark web, this landscape is expansive and complex. And this enormous repository of data, together with the anonymity it effectively provides, poses serious difficulties for enforcement and security agencies.

CONCLUSION

An anonymous area of the web known as the dark web, which may draw users in need of anonymity but serves criminal activities. The anonymity afforded to users means that they can operate without being able to trace their digital footprints, and it is thus a hotspot for child pornography as well as arms trafficking drug trafficking & onion cloning. The anonymity of the dark web encourages criminal exchanges. Many of the attacks carried out via this platform demand a ransom paid in Bit coin, due to its alleged anonymity and great traceability. Although it is also used by governments, for secure communications and operations requiring anonymity, the dark web has a largely negative social image due to its association with illegal activities. The dark web is an ecosystem of tools and technologies that support both legitimate, but especially illegal activities: Specialized Browsers Tools (e.g. Tor) accessing the dark web by sending your traffic through a cascade of computer servers, encrypting all communications at each step of the trip, would prevent anyone from discovering where you are going on the Internet. The vulnerabilities in the software and systems are exploited to get access, attack & steal data.

These are platforms that facilitate the exchange of illegal goods and services, such as drugs, weapons, or hacked information. Dark Web offers anonymity, and that is the only thing that it has to offer. This allows those who seek to regain privacy and freedom from the eyes of a global spy network some measure of relief, but it also allows criminals a way to minimize chances of being caught. And thus, the dark web is as great or terrible as its users choose to make it. It can be used for beneficial purposes, providing safety channels of communication and point's access to information in repressive environments, or detrimental purposes just the same, enabling usuries, criminal activity and even the destruction of our security.

REFERENCES

1. Chertof, M. (2017). A public policy perspective of the Dark Web. Journal Cyber Policy, 2(1), 26–38.
2. Ciancaglini, V., Balduzzi, M., & Goncharov, M. [Online]. Retrieved December 20, 2019, from https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor .
3. Mirea, M., Wang, V., & Jung J. (2019). The not so dark side of the dark net: a qualitative study. Security Journal, 32, 102–118.
4. Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the dark net: A qualitative study. Security Journal, 32, 102–118.
5. Çalışkan, E., Minárik, T., & Osula, A.-M. (2015). Technical and legal overview of the tor anonymity network. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.
6. "PGP Encryption." [Online]. Retrieved December 16, 2019, form https://www.technadu.com/pgpencryption-dark-web/57005/.
7. "Onion Routing." [Online]. Retrieved December 16, 2019, from https://www.geeksforgeeks.org/onionrouting/
8. "Types of Relays." [Online]. Retrieved December 14, 2019, from https://community.torproject.org/relay/types-of-relays/ .
9. "TOR Nodes List." [Online]. Retrieved December 20, 2019, from https://www.dan.me.uk/tornodes.
10. "Welcome to the Tor Bulk Exit List exporting tool." [Online]. Retrieved December 20, 2019, from https://check.torproject.org/cgi-bin/TorBulkExitList.py .
11. "Relay Search." [Online]. Retrieved December 16, 2019, from https://metrics.torproject.org/rs.html.
12. Rudesill, D. S., Caverlee, J., & Sui, D. (2015). The deep web and the darknet: A look inside the internet's massive black box. Ohio State Public Law Working Paper No. 314.
13. Naseem, I., Kashyap, A. K., & Mandloi, D. (2016). Exploring anonymous depths of invisible web and the digi-underworld. International Journal of Computer Applications, NCC (3), 21–25.
14. Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. International Journal of Drug Policy, 24(5), 385–391.
15. Foltz, R. (2013). Silk Road and migration. In: Encyclopedia of global human migration. https://doi.org/10.1002/9781444351071.wbeghm484 .
16. Lacson, W., & Jones, B. (2016). The 21st century Dark Net market: Lessons from the fall of Silk Road. International Journal of Cyber Criminology, 10(1), 40–61.
17. Finklea, K. (2017) Dark web report published by Congressional Research Service.
18. "Types of Attacks." [Online]. Retrieved December 16, 2019, from https://www.rapid7.com/funda mentals/types-of-attacks/.
19. Cambiaso, E., Vaccari, I., Patti, L., & Aiello, M. (2019). Darknet security: A categorization of attacks to the TOR network. In: Italian Conference on Cyber Security.
20. Evers, B., Hols, J., Kula, E., Schouten, J., Toom, M. den, Laan R. M. van der, Pouwelse J. A. (2015). "Thirteen years of tor attacks". [Online]. https://github.com/Attacks-on-Tor/Attacks-on-Tor . Accessed 18 Nov 2019.
21. Nasr, M., Bahramali, A., & Houmansadr, A. (2018) "DeepCorr: Strong fow correlation attacks on tor using deep learning". In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1962–1976).
22. Zillman, M. P. (2015). Deep Web Research and Discovery Resources 2015. [Online]. Available: https://www.llrx.com/2019/01/deep-web-research-and-discovery-resources-2019/ . Accessed 15 Nov 2019.
23. "Distributed Denial of Service Attack." [Online]. Retrieved March 18, 2019, from http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=16438&view=map .
24. Schäfer, M., Fuchs, M., & Engel, M. (2019). BlackWidow : Monitoring the dark web for cyber security information. In: Proceedings of the 11th international conference on cyber confict (CyCon), 1–21.

25. Chertof, M., & Simon, T. (2015). The impact of the dark web on internet Governance and cyber security" Global Commission on Internet Governance. Paper Series No. 6.
26. “Dark Web.” [Online]. Retrieved November 15, 2019, from https://www.fas.org/sgp/crs/misc/R44101 .
27. Satterfeld, J. “FBI Tactic in National Child Porn Sting under Attack.” [Online]. Retrieved November 20, 2019, from http://www.usatoday.com/story/news/nation-now/2016/09/05/fbi-tactic-child-pornstingunder-%0Aattack/89892954/.
28. “Confrmation Attack.” [Online]. Retrieved December 10, 2019, from https://blog.torproject.org/torsecurity-advisory-relay-early-traffic-confrmation-att 29. Ashford, W. “Firms face targeted bespoke cyber-attacks, dark web study reveals.” [Online]. Retrieved December 10, 2019, from https://www.computerweekly.com/news/252464660/Firms-face-targetedbespoke-cyber-attacks-dark-web-study-reveal