WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# "Going Dark" - The Internet Behind The Internet

***Gowda Siddesh Basavaraju[1], Sai Sudheer K[2], Keshavram D[3]***

[1]Dept. of Electronics and Communication Engineering T. John Institute of Technology ,Karnataka, India, siddeshgowda613@gmail.com
[2]Dept. of Electronics and Communication Engineering T. John Institute of Technology, Karnataka, India, saisudheer2609@gmail.com
[3]Dept. of Electronics and communication Engineering T. John Institute of Technology, Karnataka, India, keshav58653@gmail.com

## Introduction :

The term "Dark Web" describes a section of the Internet where users can browse anonymously and where material has been purposefully hidden. A application that functions similarly to a web browser or search engine must be installed in order to access the DW and its content. The application with the greatest level of popularity is The Onion Browser (TOR) (MEDI@4SEC D1.1). Thus, encryption is the characteristic that sets the Dark Web apart from the open web. In theory, encryption is neither morally nor legally questionable, but in practice, a large portion of the activities that individuals in liberal democracies engage in on the Dark Web is either immoral or unlawful. The Dark Web is home to a wide range of websites and forums that promote immoral and unlawful behavior. These include money-laundering websites, extremist websites, and forums where information about child sexual abuse is shared. Other criminal activities include contract murders, drug sales, and counterfeit products. All of these actions are acceptable targets for law enforcement, and encryption makes them more difficult to stop and punish while also making them simpler to carry out. On the other hand, not just criminals utilize the dark web. Law enforcement, the military, journalists, political dissidents, and activists all benefit from the security and anonymity that encryption provides.

The deep web, or the portions of the internet that search engines do not index or index, is sometimes mistaken with the black web. It is unclear when the real dark web initially appeared, however the phrase "dark web" first appeared in 2009.A standard web browser can access the data on the surface web, which is all that many internet users utilize. A little portion of the deep web is made up of the dark web, to which access to its content needs specialized software. This misconception began, at the very least, in 2009. Since then, despite suggestions that they be used differently, the two phrases have frequently been used interchangeably, particularly in reporting on Silk Road. Only networks designed expressly for the dark web, like Tor ("The Onion Routing" project"), may access the black web, sometimes referred to as darknet websites. Users of the darknet frequently utilize the Tor browser, and websites that are accessible through Tor are distinguished by the ".onion" domain. Users using Tor browsers may access the dark web anonymously by creating encrypted entry points and tunnels for them.

## What is The Dark Web :

A portion of the internet that is encrypted and hidden from public view is known as the "dark web." Another name for it is the darknet.

The dark web is frequently linked to illicit activities like the selling of cyber-arms, guns, and counterfeit money, as well as drug trafficking and data breaches. But there are legitimate uses for the dark web as well, as when government organizations exchange sensitive data. Political dissidents and other individuals who wish to keep specific information secret can also utilize it.

The term "Dark Web" refers to a collection of publicly accessible websites that are concealed but purposefully conceal their IP address or Internet Protocol (IP) (Finklea, 2017). Anyone with access to the Internet can view these websites, but it might be challenging to identify the server that the related site is hosted on and to obtain the server specifics. You may achieve the idea of the Dark Web by using anonymizing technologies. The Onion Router (TOR) is one well-liked tool. The Dark Web offers advantages and disadvantages, since it is well-liked for user safety as well as the illicit market (Finklea, 2017). The majority of goods and services available on the Dark Web are utilized for evil intent. Many other types of networks, run by both private and public entities, are part of the Dark Web. These vary from small, friend-to-friend/peer-to-peer networks to major, well-known networks like Freenet, I2P, and TOR (Finklea, 2017). As the internet's vulnerability to tracking and surveillance became more apparent in the 1990s, David Goldschlag, Mike Reed, and Paul Syverson at the U.S. Naval Research Lab (NRL) sought to determine whether it was possible to establish internet connections that conceal user identities from network monitors (TOR Network, 2019). Their response was to develop and implement the initial onion routing research designs and prototypes (TOR Network, 2019).

Onion routing was designed to operate on a decentralized network from the start in the 1990s (TOR Network, 2019). To optimize transparency and separation, the software had to be free and open, and the network had to be run by organizations with a variety of interests and trust philosophies (TOR Network, 2019). The primary intent behind developing this project was to protect users' online privacy and identity. Web-based covert services fall into several categories, such as: drugs, fraud, gambling, hacking, and illegal hosting. The majority of Dark Websites effectively disguise themselves and are not readily accessible through a standard search engine query. They can only be accessed if the user is aware of the addresses of such websites. To avoid being discovered by governments and law enforcement, illicit goods are sold on the black market over the Dark Web. In order to shield users

from assaults or monitoring and to maintain communication privacy, the Dark Web is also utilized in various contexts, such as for whistleblower communication. However, because it offers complete anonymity, the Dark Web is largely utilized in illicit markets.

## Investigating dark websites :

According to Guccione (2019), law enforcement agents are becoming more adept at locating and prosecuting the proprietors of websites that offer illegal products and services. Shudders ran through the network when a group of cyberpolice from three different nations took down AlphaBay, the main source of illicit goods on the Dark Web, in the summer of 2017. (Guccione, 2019). However, a large number of these black market vendors just moved on. The Department of Justice claims that it is "impossible for law enforcement" to pursue criminal suspects because of the Dark Web's usage by criminals to anonymize communications (Ghappour, 2017).

Finding the suspect's device or computer is the most important stage in computer crime cases in order to identify the offender and gather evidence for a strong prosecution (Ghappour, 2017). Investigators won't have any proof linking virtual criminal activity to a specific individual if the suspect doesn't have access to their laptop (Ghappour, 2017). Traditional investigative techniques depend on coercing and obtaining agreement from third people in order to get data (Ghappour, 2017). Compulsory process is used to gather digital evidence when it is under the custody of an entity or person subject to personal jurisdiction in the United States (Ghappour, 2017).

Formal and informal law enforcement cooperation methods are utilized to get digital evidence when it is beyond U.S. jurisdiction—for example, when it is in the control of a company that does not have assets or a physical presence in the country (Ghappour, 2017). Criminals in the twenty-first century are depending more and more on the Internet and cutting-edge technology to carry out their illegal activities (Finklea, 2017). For example, criminals may readily use the Internet to commit more conventional crimes, such sex trafficking and the distribution of illegal narcotics (Finklea, 2017). Furthermore, they take use of the digital sphere to enable crimes that are frequently fueled by technology, such as identity theft, credit card fraud, and theft of intellectual property (Finklea, 2017). According to the FBI, high-tech crimes are among the most serious ones that the US faces (Finklea, 2017).

### *Why Is the Dark Web So Dangerous?*

The Dark Web's capabilities are frequently utilized by cybercriminals and other bad actors for different illicit purposes. Dark Web forums and marketplaces are hubs for illicit activity where criminals trade illicit goods and services.

On these black markets, criminals and con artists sell a variety of illegal goods, including stolen and counterfeit data.

private information. (Often known as personally identifiable information, or PII) Full names, residential addresses, phone numbers, dates of birth, Social Security numbers (SSN), compromised email addresses, and a plethora of other information that may be used to identify a specific person are included in this.

financial information. Credit card numbers, usernames, passwords, cryptocurrency account credentials, bank and insurance information, and much more have all been stolen.

login credentials for an online account. usually consisting of login and password combinations that provide access to several accounts, such as those on social media, ride-sharing platforms, streaming video services, and paid professional services. There is also demand for logins to antivirus software and genetic testing.

health-related information. (Often known as personal health information, or PHI) This includes test results, billing information, biometric data (such as fingerprints and facial photos), medical history, medications, and other private information. This can lead to medical identity theft or even fingerprint identity theft in the wrong hands.

private company information. contains confidential data on patents, intellectual property, competitive intelligence, and other operational specifics.

Forged data. Most notably, bank drafts, counterfeit passports, and stolen IDs and driver's licenses

These underground marketplaces not only provide access to a plethora of newly discovered cyberthreats and viruses, but they also sell illicit substances, employ hitmen, and personal information obtained from data breaches and other cyberattacks and online frauds. At its height, serving over 100,000 purchasers, Silk Road was the most well-known Dark Web bazaar.

Established by Ross Ulbricht in 2011, the website rose to prominence as the go-to dark market, particularly for drug dealers. Silk Road was taken down by the FBI in 2013, however before law authorities pulled it down permanently, version 2.0 was briefly restored to the internet.

Ross Ulbricht was found guilty of three further counts and given two life terms in jail. Over $1 billion worth of bitcoin was confiscated by the US authorities during the takedown operation and in the ten years that followed.

### *Services That Cybercriminals Can Access Through the Dark Web*

Even though you might think that personal information is priceless, hackers will exchange it for a few bucks on the Dark Web's underground markets.The average cost of credit card theft is $150 for data with a value up to $1,000, but stolen login credentials for online banking accounts with a minimum balance of $100 only fetch $40.

The Dark Web even has marketplaces with review and ranking systems so that purchasers may find "reliable" sellers. It seems sense that these underground markets are seeing a sharp increase in supply given all of these characteristics plus the allure of cybercrime profits, as indicated by the Dark Web Price Index.

In addition to selling hacked accounts and personal information, fraudsters also market: Pre-made software vulnerabilities (exploit kits). Toolkits are used by hackers to target system weaknesses in order to propagate malware.

harmful program (malware) that is ready to use. Ransomware, data theft, keyloggers (which track every key hit on a system), spyware, adware, rootkits (which are notoriously hard to identify and remove), Trojan horses, and worms (which have the ability to replicate themselves).

Cybercrime as a service. a subscription-based business model that lets cybercriminals rent the gear and software they need to launch attacks, along with malicious malware, a distribution network, a variety of targets, technical assistance, and a dashboard for project management.
flaws in software. Unbeknownst to the program developer, fraudsters can leverage this to stealthily penetrate businesses.
Access to botnets, or networks of infected devices. The computer power that malevolent hackers require to launch their assaults.
denial of service distributed (DDoS). Services that overwhelm victims' systems with so much traffic by the deployment of massive botnets that the victims' systems go down and their services are no longer available.
Training for cybercriminals. tutorials, manuals, and other materials that help terrible actors become more proficient in a variety of roles.
Financial fraud (money muling). allows con artists to spread the money they take from their victims through extortion, theft, or other means, and convert it into currency that is easy to disappear.

## Dark Web Activities :

***Social networks***

There are new social media sites that are sprouting on the dark web that resemble the World Wide Web; these are called the Dark Web Social Network (DWSN). Similar to other social networking sites, DWSN allows users to create personalized pages, add friends, comment on topics, and write in discussion boards. In order to solve issues with the traditional platforms and maintain service throughout the whole World Wide Web, Facebook and other traditional social media companies have started to create dark-web versions of their websites.In contrast to Facebook, the DWSN's privacy policy mandates that members maintain their anonymity and provide no personal information at all.

***Acts of terrorism***

Even while terrorist groups started using the internet in the 1990s, the anonymity, unregulated nature, social interaction, and ease of accessibility of the dark web eventually drew them in. These organizations have been using the dark web's chat rooms as an inspiration for acts of terrorism.Even "How To" guidelines have been produced by groups, instructing people on how to become terrorists and conceal their identity.
Funding, guidance, and most critically, terrorist propaganda found a home on the dark web. Anonymous transactions were made possible with the invention of Bitcoin, enabling funding and donations from a distance. Terrorists were now able to finance the purchase of weapons by accepting Bitcoin.[65] An person by the name of Ahmed Sarsur was accused in 2018 for trying to use the dark web to buy explosives and employ snipers to help Syrian terrorists in addition to trying to give them money.

***Money and deception***

According to Zebryx Consulting's president and CEO, Scott Dueweke, most criminal activities are funded by Russian electronic money, specifically WebMoney and Perfect Money. Flashpoint was awarded a $5 million investment in April 2015 to assist its clients in obtaining intelligence from the dark and deep web.Along with trade websites for Bitcoin and PayPal, carding forums abound, as do fraud and counterfeiting businesses. Numerous of these websites are frauds as well.There are several ways to commit phishing, including using cloned websites and other scam sites. Darknet markets are frequently promoted using phony URLs.

***hacker networks and services***

Numerous hackers offer their skills both individually and in groups.These communities include TheRealDeal darknet market, xDedic, hackforum, Trojanforge, Mazafaka, and dark0de. Some have a history of tracking down and intimidating suspected pedophiles. Through the dark web, cybercrimes and hacking services for banks and financial institutions have also been made available. Numerous governmental and corporate groups have attempted to keep an eye on this behavior, and the Procedia Computer Science journal has examined the instruments employed. The dark web has also been used to launch DNS distributed reflection denial of service (DRDoS) assaults on an Internet-scale. There are a lot of phony onion websites out there that ultimately offer downloads of trojan horses or backdoor-infected software.

***Services for Bitcoin***

Bitcoin is a popular cryptocurrency that is utilized in dark web marketplaces because of its versatility and relative anonymity. People can conceal both their identities and their goals while using Bitcoin. Using a digital currency conversion service to convert Bitcoin into virtual currency used in online games (like World of Warcraft gold coins) and then converting it back into fiat money was a popular method. Tumblers and other bitcoin services are frequently accessible on Tor, and some of them—like Grams—also provide darknet market integration.
A study conducted by ESSEC research fellow Jean-Loup Richet in collaboration with the UN Office on Drugs and Crime revealed emerging patterns in the usage of Bitcoin tumblers for money laundering.
Owing to its significance in the digital realm, Bitcoin has grown in popularity as a tool for individuals to con businesses. Since the introduction of Bitcoins in 2014, more than 140 assaults against businesses have been carried out by cybercriminal groups like DDOS"4". Along with cyber extortion, these attacks have spawned additional cybercriminal organizations.

***Darknet Sales***

Commercial darknet markets accept Bitcoin as payment and function as middlemen for transactions involving illicit items. Since the Silk Road and Diabolus Market gained notoriety and were taken over by law enforcement, both marketplaces have received a great deal of media attention. One of the earliest dark web markets to appear in 2011 was Silk Road, which made it possible to trade weapons and resources for identity theft. Users of these marketplaces are not protected in any way, and authorities have the right to close them down at any moment. These markets close, but others keep popping up in their stead. There were at least 38 active dark web markets as of 2020. These online markets, which resemble Craigslist or eBay, allow consumers to communicate with merchants and provide reviews of the goods they have purchased.

***Fake news and unreliable sources***

Hitmen for hire and crowdfunded killings have been reported, however they are thought to be complete frauds. Homeland Security investigations (HSI) detained Silk Road founder Ross Ulbricht for his website and reportedly for hiring a hitman to kill six people, however the accusations were ultimately dropped. There is a persistent belief that live murder may be found on the dark web. Though the evidence suggests that all recorded occurrences of the urban legend and Japanese cartoon of the same name are fake, the phrase "Red Room" was born.
YouTubers Obscure Horror Corner reviewed the independent game Sad Satan on June 25, 2015, claiming to have discovered it on the dark web. The reported version of events is called into question by a number of contradictions in the channel's reporting. Numerous websites provide threat intelligence analysis and monitoring of the deep and dark webs.

## The Dark Web's Monitization by Criminals :

committing identity theft and other forms of financial crime using stolen personal data.
using private information that has been stolen to threaten businesses and people, including threatening to post it on the Dark Web.
using financial data to take out illegal loans, empty bank accounts, pay for products and services without authorization, and get other illicit financial gains.
To access more accounts, take more data, and resell it on the Dark Web for a profit, employ username-password combinations in automated, mass assaults.
Infect devices with malicious software, such as ransomware, to either collect more data, utilize it in other assaults, or demand payment from victims.
Interrupt the operations of a company to lose money, ruin its reputation, and incur expensive long-term consequences.
Steal and resell intellectual property to rival companies, breach corporate email accounts of corporations, or hold their systems ransom until a large ransom is paid.
Because it is simpler to integrate malware and compromised infrastructure with stolen data, specialized criminal gangs prosper. This implies that even less experienced malevolent hackers may conduct successful cyberattacks and develop profitable ventures.
The Dark Web is a hub for illegal activity because, up until a point, it provides the anonymity needed for hackers and fraudsters to remain undiscovered.

## Monitoring the dark web :

The notion that the dark web supports civil rights such as "free speech, privacy, and anonymity" has been proposed.There are government agencies and prosecutors that worry that it's a sanctuary for illicit activities. Applications utilizing essential internet properties that offer anonymity and privacy are found on the deep and dark web. Targeting certain private web behaviors that are regarded unlawful or susceptible to internet restriction is known as policing.
Police usually utilize the suspect's IP (Internet Protocol) address when looking into someone online, however since Tor browsers provide anonymity, this is not feasible.Consequently, law enforcement has utilized several other strategies to detect and apprehend those involved in illicit activities on the dark web. Open Source Intelligence, or OSINT, refers to a set of lawful data collecting techniques that obtain information from public sources. Officers can obtain tidbits of information that can assist them learn more about interactions occurring in the dark web by using OSINT technologies designed specifically for the dark web.
It was revealed in 2015 that Interpol now provides a specific training curriculum for the dark web that includes technical details on Tor, cybersecurity, and simulated takedowns of darknet markets. The establishment of a "Joint Operations Cell" with an emphasis on cybercrime was announced in October 2013 by GCHQ and the UK's National Crime Agency. This squad was assigned to deal with cybercrime in November 2015, including child exploitation on the dark web.The Congressional Research Service published a comprehensive study on the dark web in March 2017, highlighting the evolving nature of information access and presentation on it. Because of its unpredictability, researchers, law enforcement, and politicians are becoming more interested in it.
Reports from August 2017 said that cybersecurity companies that monitor and study the dark web for shops and banks frequently communicate their findings with law enforcement organizations, including the FBI, "when possible and necessary" in relation to illicit material. One especially strong model for crime-as-a-service is said to exist in the Russian-speaking underground.

REFERENCES :

[1] Jamie, B. (2014). The Dark Net.

[2] Lightfoot, S., & Pospisil, F. (2017). Surveillance and privacy on the deep Web. ResearchGate, Berlin, Germany, Tech. Rep.
[3] Senker, C. (2016). Cybercrime & the Dark Net: Revealing the hidden underworld of the internet. Arcturus Publishing.
[4] Henderson, L. (2022). Tor and the dark art of anonymity (Vol. 1). Lance Henderson.
[5] Diodati, J., & Winterdyk, J. (2021). Dark Web: The Digital World of Fraud and Rouge Activities. In Handbook of Research on Theory and Practice of
Financial Crimes (pp. 477-505). IGI Global.
[6] Gehl, R. W. (2018). Weaving the dark web: legitimacy on freenet, Tor, and I2P. MIT Press.
[7] Ozkaya, E., & Islam, R. (2019). Inside the dark web. Crc Press.
[8] Beckstrom, M., & Lund, B. (2019). Casting light on the Dark Web: A guide for safe exploration. Rowman & Littlefield.
[9] Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. The British Journal of Criminology, 60(3), 559-578.
[10] Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.
[11] Davenport, D. (2002). Anonymity on the Internet: why the price may be too high. Communications of the ACM, 45(4), 33-35.