International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

# CYBER CRIME INVOLING DARKNET

*Divya Ramesh Gorivale*
Guide: Asst. Proff. Bindy Wilson
Keraleeya Samajam'sModel College, Khambalpada, Dombivli(East)

**Abstract:**

World Wide Web or www are already known and being used widely in this millennium. We would like to search information, watching video or movies, socialize through online platform such as Facebook, Instagram or Twitter and do almost everything at any time using www. However, most of us doesn't know that the normal use of www is just about 30% of the entire www. The much larger of www usage is on its deep web which is including the dark web. What inside dark web? The dark web contains many illegal activities and illicit materials as well as criminal intervention. It is becoming the nest for the cyber criminals whereby it is a place for all cyber criminals join and gather to spread their seed of darkness. Hackers, drug dealer, terrorist, virus innovators, sex maniacs, pedophiles, stalkers, cyber bullies and all unimaginable person are there. Virus, malware, phishing and identity theft was wandering around every time. A small mistake will cause vital consequences, you can be stalked, threatened, stole even murdered if you not be careful. The dark web usually have 3 compositions, browser, search engine and website. It is similar with the surface web but using a different tools and configurations. One of the issue wondering in the dark web is how the commerce happen in there, most of it are using bitcoins as their premier transection and also a few method which we will be discussed further. Dark web is the no 1 place for hackers, they are wandering around and do their actions to analyze, study and testing their capabilities. So, it is very suitable that dark web is the nest for them. Do not confuse between Deep Web and Dark Web, dark web is a part deep web and deep web is a larger definition from dark web. To get into dark web you have to use special browser named The Onion Router (TOR), you just need to download and follow the instruction and it is free! Do not mess with something that you don't understand, you must learn to protect yourself when you enter the dark web. Policymakers must gain an understanding of the Dark Web in order to engage intelligently in the debate and enact effective dark web policy.

**Keywords:** ***www, dark web, deep web, browser, search engine, website, commerce, hackers, TOR.***

## I. INTRODUCTION

As for definition, Dark Web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browsers and it uses layered encryption

Networks. Most of the dark web contents are illegal material which usually being used for criminal activities. Dark web can be considered as a host of illicit material. A research done by Daniel Moore and Thomas Rid from King's College in London found that 57% of Dark Web material is illicit.

The websites that we generally use and access, such as this one is on the “clearnet”. It’s not public knowledge, but the clearnet sites, such as Facebook, Google, Youtube, blogs etc amount to only for around 5% of the total internet! The other 90-95% of the internet is unindexed and hence is termed as the Deep Web. Also, most of the general public never gets access to the unindexed content or the Deep web, whatever we need, can almost always be found on the clearnet and easily too via search engines and most people are satisfied with that.

The dark web content usually exists on personal encrypted networks or peer-to-peer configurations. It can only be accessed using special software and decryption tools

such as a Tor browser and most of the websites on the Dark Web contain fishy content which need that kind of encryption. These websites cannot be visited using search engines or traditional browsers as their address are encrypted and cannot be traced using conventional methods. The dark web was created by the US government to allow spies to exchange information completely anonymously. US military researchers developed the technology, known as Tor in the mid-1990s and released it into the public domain for everyone to use. The reason was so that they could stay anonymous - it would be harder to distinguish the government's messages between spies if thousands of other people were using the same system for lots of different things. Tor now hosts roughly 30,000 hidden sites.

The Dark Web sites generally use the Tor encryption tool to mask their identities due to which they can keep their activities hidden. The tool basically functions just

like a VPN and consistently randomizes the host’s location to a different country so it’s almost impossible to detect where the user is.Tor-encrypted websites can easily be accessed using a Tor browser. It provides secrecy for both ends – the website and the visitor both. The IP addresses using the browser bounce constantly to random locations while getting concealed under several layers of encryption.The Dark Web remains incredibly attractive to internet users for a wide range of reasons. The enshrouded nature and complex methodology required to access this world have effectively made it a secret world, full of salacious activity, black

markets, sights, and perks limited to a select few.

The websites can be visited by any user in any part of the world by simply inputting the address in their Tor browser, however, it is difficult to spot the location or identity of the websites. Depending on how

actionable the Dark Web-based activity is, it can be extremely dangerous if the user's identity gets revealed.

## II. WHAT INSIDE DARK WEB

Dark web sites look pretty much like any other site, but there are important differences. One is the naming structure. Instead of ending in .com or .co, dark web sites
end in onion. That's "a special-use top level domain suffix designating an anonymous hidden service reachable via the Tor network," according to Wikipedia. Browsers
with the appropriate proxy can reach these sites, but others can't.

You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you
break into other people's computers. Buy login credentials to a $50,000 Bank of America account for $500. Get $3,000 in counterfeit $20 bills for $600. Buy seven
prepaid debit cards, each with a $2,500 balance, for $500 (express shipping included). A "lifetime" Netflix premium account goes for $6. You can hire hackers to attack computers for you. You can buy usernames and passwords.

As summery, dark web can be considered as the nest of most cybercrimes actively running in it even an imaginary crime also in the dark web.

Dark web is the nest for:

- Various types of drugs.
- Weapons.
- Hacked software.
- Stolen credit cards and bank details.
- Fake documents such as Passports and Visas.
- Hacking services.
- In some cases, you can even hire Hitman and contract killers.

Apart from darknet markets, the dark web also is a hub for things such as child pornography, and red rooms. Red rooms are rooms where real human beings and animals are tortured, raped and even murdered, and all of this is streamed live for the audience, at a price. In some red rooms even requests from the audience is taken on how to
torture and kill the victims.

But not everything is illegal, the dark web also has a legitimate side. For example, you can join a chess club or BlackBook, a social network described as the "the Facebook of Tor."

## III. DARK WEB COMPOSITION

All of this activity, this vision of a bustling marketplace, might make you think that navigating the dark web is easy. It isn't. The place is as messy and chaotic as you would expect when everyone is anonymous, and a substantial minority are out to scam others.

A. Dark web browser

Accessing the dark web requires the use of an anonymizing browser called TOR (The Onion Router) or I2P (Silk Road Reloaded) [7] but mostly are using TOR. The Tor
browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable
and untraceable. Tor works like magic, but the result is an experience that's like the dark web itself: unpredictable, unreliable and maddeningly slow.

B. Dark web search engine

Dark web search engines exist, but even the best are challenged to keep up with the constantly shifting landscape. The experience is reminiscent of searching the web in the late 1990s. Even one of the best search engines, called Grams, returns results that are repetitive and often irrelevant to the query. Link lists like The Hidden Wiki are another option, but even indices also return a frustrating number of timed-out connections and 404 errors. Currently the most famous dark web search engine is Duck Duck Go.

C. Dark web sites

Dark web sites look pretty much like any other site, but there are important differences. One is the naming structure. Instead of ending in .com or .co, dark web sites end in .onion. That's "a special-use top level domain suffix designating an anonymous hidden service reachable via the Tor network," according to Wikipedia. Browsers with the appropriate proxy can reach these sites, but others can't. Dark web sites also use a scrambled naming structure that creates URLs that are often impossible toremember. For example, a popular commerce site called Dream Market goes by the unintelligible address of "`q 1`". Many dark websites are set up by scammers, who
constantly move around to avoid the wrath of their victims. Even commerce sites that may have existed for a year or more can suddenly disappear if the owners decide to
cash in and flee with the escrow money they're holding on behalf of customers.

Law enforcement officials are getting better at finding and prosecuting owners of sites that sell illicit goods and services. In the summer of 2017, a team of cyber
cops from three countries successfully shut down AlphaBay, the dark web's largest source of contraband, sending shudders throughout the network. But many merchants simply migrated elsewhere.

The anonymous nature of the Tor network also makes it especially vulnerable to distributed denial of service attacks (DDoS) [7], said Patrick Tiquet, Director of Security & Architecture at Keeper Security, and the company's resident expert on the topic. "Sites are constantly changing addresses to avoid DDoS, which makes for a very dynamic

environment," he said. As a result, "The quality of search varies widely, and a lot of material is outdated."

## IV. COMMERCE ON THE DARK WEB

The dark web has flourished thanks to Bitcoin, the cryptocurrency that enables two parties to conduct a trusted transaction without knowing each other's identity.

Bitcoin has been a major factor in the growth of the dark web, and the dark web has been a big factor in the growth of bitcoin.

Nearly all dark web commerce sites conduct transactions in bitcoin or some variant, but that doesn't mean it's safe to do business there. The inherent anonymity of the place attracts scammers and thieves, but what do you expect when buying guns or drugs is your objective?

Dark web commerce sites have the same features as any eretail operation, including ratings/reviews, shopping carts and forums, but there are important differences. One is quality control. When both buyers and sellers are anonymous, the credibility of any ratings system is dubious. Ratings are easily manipulated, and even sellers with long track records have been known to suddenly disappear with their customers' crypto-coins, only to set up shop later under a different alias.

Most e-commerce providers offer some kind of escrow service that keeps customer funds on hold until the product has been delivered. However, in the event of a dispute don't expect service with a smile. It's pretty much up to the buyer and the seller to duke it out. Every communication is encrypted, so even the simplest transaction requires a PGP key.

Even completing a transaction is no guarantee that the goods will arrive. Many needs to cross international borders, and customs officials are cracking down on suspicious packages. The dark web news site Deep.Dot.Web teems with stories of buyers who have been arrested or jailed for attempted purchases.

## V. STAYING ON TOP OF THE HACKER UNDERGROUND

Keeper's Patrick Tiquet checks in regularly because it's important for him to be on top of what's happening in the hacker underground. "I use the dark web for situational awareness, threat analysis and keeping an eye on what's going on," he said will. "I want to know what information is available and have an external lens into the digital assets that are being monetized – this gives us insight on what hackers are targeting."

During the Arab Spring, revolutionaries used the Dark Net in order to avoid being discovered by their oppressive governments. These groups are aided by denizens of the

Dark Web who support the idea of freedom of expression and the transparency of government. The hacker group "Anonymous" almost routinely breaks into protected systems, and during the Arab Spring assisted the protestors by supplying methods of

circumventing the government's controls on the Internet and maintaining the channels of communication. Although "Anonymous" is known for breaking websites through distributed denial of service attacks or for revealing personal information, their early actions epitomized the style of the first "hackers."

If you find your own information on the dark web, there's precious little you can do about it, but at least you'll know you've been compromised. Bottom line: If you can tolerate the lousy performance, unpredictable availability, and occasional shock factor of the dark web, it's worth a visit. Just don't buy anything there.

Zero-Day, Zero-day refers to the vulnerabilities or holes in software and the exploits or attacks that use malicious codes in these software vulnerabilities to plant a virus, Trojan horse, or other malware. The term "zero-day" refers to the number of days the hole in the software has been known by the creator or vendor. Since zero-day vulnerabilities are unknown to the software creator and vendors, they are very dangerous to computers because malware or software updates do not know where or how to protect you from being hacked from these holes. This is what makes zero-day exploits so valuable to hackers, they are very powerful, easy to hack when found, and rare to come by.

Figure 2: Internet Iceberg [2]

| | THE SURFACE WEB | THE DEEP WEB | THE DARK WEB |
|---|---|---|---|
| How to Access | Traditional search engine | Requires password, encryption, or specialty software | Requires Tor Project or similar to view |
| Includes | All indexed web pages | All unindexed webpages | Subset of unindexed webpages inside the deep web |
| Size | Approximately 4.47 billion pages | Massive, likely 4-5x larger than the Surface web | A subset of the Deep Web, but unmeasurable in size |
| Uses | Email, social media, video, legitimate business websites, etc. | Usually used for legit purposes that require anonymity | Sometimes used for illegal activities |
| Who uses it? | Anyone with an internet connection | Whistleblowers, journalists, etc. | Hackers, sellers & buyers of illegal merchandise |
| Can be browsed anonymously? | No, nearly all activity can be seen by your ISP. | Usually, especially if you use a VPN to access. | With precautions, yes. |

Table 1 [4]

## VI. DEEP WEB VS DARK WEB

Note that the "Deep web" and the "Dark web" are two separate things, basically, the "Dark web" is a deeper but smaller part of the deep web.

The terms between the two are often considered to be the same because of the confusion of the media, it is not the same thing. Deep Web refers to all sites that

search engines cannot search. For that, Deep Web includes the Dark Web.

In addition to the Dark Web, Deep Web includes all database users, browsing websites, forums for site registration users, pages for online transaction payments and
other sites available on the background website and not necessarily for ordinary users to know. However, all the contents of the Deep Web are much larger than what's
on the web surface.

The confusion posed by some of the media that cannot distinguish between Dark Web and Deep Web makes Deep Web seem to be filled with prohibited content, much the same as the Dark Web. However, Deep Web is indispensable for purposes such as online transaction security between users and banks as well as confidential information for use by government agencies.

Here are the differences between the Deep web and the Dark Web:

 Dark web is a “part” of the Deep Web. Deep web is the larger set while the dark web is just a subset.

 Every dark web content is automatically also deep web content (because it’s illegal, so it’s not indexed), but not all deep web content can be termed as being of Dark web.

 Accessing the deep web isn’t always illegal, you may believe in conspiracy theories or things like that which may be unindexed and still legal, while everything and anything on the dark web is illegal.

 The deep web also exists on the clearnet, as almost every site has codes and other elements which aren’t indexed, but the dark web doesn’t exist on the clearnet, and exists
solely on the “Tor” network (onion network).

Have you ever thought of the internet as an iceberg? There are some good reasons to do so. What we can see is only a minor part of the total internet. Underneath is an invisible part, which forms the majority of the internet sites worldwide. We call this invisible part is the ‘deep web’, with part of it being the ’dark web’, deep and dark, like the underwater part of an iceberg.

Tor was originally developed by a US government agency through the Office of Naval Research and Defense Advanced Research Projects Agency. It can make its users anonymous through what is called "onion routing". Data transmitted through this network will be through various types of routers so it becomes difficult to keep track
of where the origin of the request was made. To navigate a website on the Dark Web using TOR encryption, the user should use the TOR browser. The IP address of both
parties, both users and site providers has gone through various levels of encryption for it to be met on the TOR network.

Due to the difficulty in identifying who is behind a website, it is very dangerous if the identity of a user has been leaked.However, not all Dark Web websites use Tor.

Some use services like I2P used by Silk Road Reloaded. In addition, I2P is another popular dark net for malware, with a few discovered samples:

Criptowall 3.0 and the Dyre Trojan.

The fundamentals for both remain the same to describe the transmission of data between the two parties.

A. How to use the Tor Browser

Technically, the process is not so complicated. Users only need to install and use Tor which can be obtained from http://www.torproject.org/ and download the
Tor Browser

Bundle which contains all necessary functions. Instructions for installation steps will be provided according to user's suitability.

Tor Browser is available for Linux, Mac and Windows, and has since been ported to mobile. If you're on Android, find OrBot or OrFox on the Google Play Store or F-Droid.
iOS users can grab Onion Browser from the Apple App Store.

B. How the TOR Browser works

Tor Browser routes all your web traffic through the Tor network, anonymizing it. Tor consists of a three-layer proxy, like layers of an onion. Tor Browser connects at
random to one of the publicly listed entry nodes, bounces that traffic through a randomly selected middle relay, and finally spits out your traffic through the third and final exit node.

Figure 3 [14]

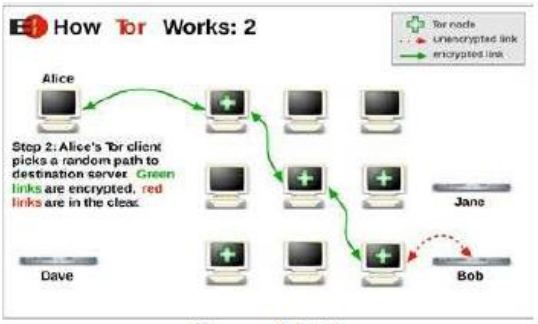

Figure 4 [14]

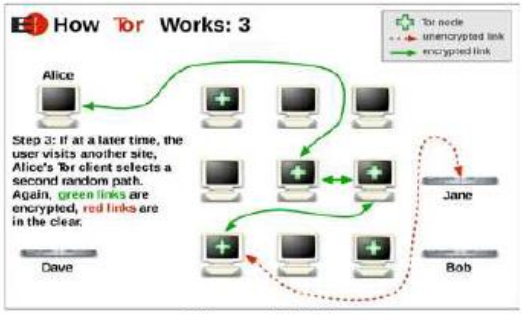

Figure 5 [14]

## VII. CONCLUSION

Nowadays, countless internet users try to enter the dark web. Some are looking for something in particular that simply can't be sourced on the regular internet, others
are simply curious and excited to search what is inside the dark web. Some of them are aware how dangerous the dark web and have their own precaution actions to protect
themselves, but most of them are know nothing and they are vulnerable to the dangerous of dark web. Do not use dark web if you don't know how to protect yourself.

In there, doesn't mean that you are not doing crime you are safe, once you enter a lot of predators are waiting you to make mistake and flopover your life.

Be careful and remember, do not mess with something that you do not understand. Knowledge yourself first before you go into dark web, because in dark web you are by
your own and you need to protect yourself every time, always take your preventive action before you enter the dark web.

In Malaysia context, it is questionable that Malaysian really aware of dark web visibility. The awareness about the dark web and it dangerous not in clear picture from
the authority. Information, analysis, statistics and study about dark web in Malaysia are still in vague, it is a great opportunity and honor if researcher do comprehensive research about the dark web in Malaysia perspective. The collaboration and result of the research can be used to prevent and control the usage as well as awareness to the public by the authority bodies.

The debate surrounding the Dark Web is by no means over. Online anonymity is a double-edged sword that must be handled delicately. As policymakers move forward, they
must monitor vigilantly the evolution of the Dark Web and ensure that enforcement.

## VIII. REFERENCES

[1] T. R. Daniel Moore, "Cryptopolitik and the Darknet," 1 Feb 2016.

[2] TheDarkWebLinks, What is the Deep Web? The Definitive Guide [2019], 2019.

[3] J. Hale, "What is the dark web? From drugs and guns to the Chloe Ayling kidnapping, a look inside the encrypted network," 2 Aug 2019.

[4] C. Sheils, "The Deep & Dark Web: What Lies Beneath The Internet's Surface?," 1 October 2019.

[5] Darren Guccione, "What is the dark web? How to access it and what you'll find," 4 July 2019.

[6] S. R. Koyande, Y. V. S. Reddy and M. Dendge, "Invisible Web," May-Jun 2018.

[7] M. G. Ionita and P. V. V. Patriciu, "Defending Against Attacks from the Dark Web - Using Neural Networks and Automated Malware Analysis," Jul 2016.

[8] E. Jardine, "The Dark Web Dilemma: Tor, Anonymity and Online Policing," Sep 2015.

[9] E. Dilipraj, "Terror in the deep and Dark web," Sep 2017.

[10] M. Chertoff, "A public policy perspective of the Dark Web," 13 Mar 2017.

[11] P. Narasimhan, "What is Agora in the dark web?," 11 Jul 2017.

[12] O. Bertrand, ""The Dark Web: What's Beneath The Tip of an iceberg?," 8 May 2017.

[13] C. R. R. M. A. S. J. G. a. L. C. Danielle LeFrancois, "Hackers and the Dark Net: A Look into Hacking and the Deep Web," vol. 5, no. 1, 2017-2018.

[14] J. Porup, "What is the Tor Browser? How it works and how it can help you protect your identity online," 15 Oct 2019.