Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue17,December 2019

A SURVEY TO DARK WEB…….!

Ms.Jayakeerthi.M[1],Jincy Rajeevan[2],Abijith .P.A[3]

Assistant Professor[1],PG Students[2,3] Department of Computer Science[1,2&3],

AJK College of Arts and Science,Coimbatore,Tamil Nadu,India[1,2&3]

Abstract— *The Internet as the complete is a network of multiple pc networks and their large infrastructure. The net is made up of accessible web sites via search engines including Google, Firefox, etc. And it is known as the Surface Web. The Internet is segmented further in the Deep Web—the content that it isn't listed and can't get admission to by conventional search engines like google and yahoo. Dark Web considers a phase of the Deep Web. It accesses thru TOR. Actors inside Dark Web web sites are anonymous and hidden. Anonymity, privacy and the opportunity of non-detection are 3 factors that are provided by unique browser inclusive of TOR and I2P. In this paper, we're going to discuss and offer outcomes about the influence of the Dark Web in different spheres of society. It is given the range of every day nameless customers of the Dark Web (using TOR) in Kosovo as well as in the whole world for a period of time. The impact of hidden services web sites is proven and outcomes are accumulated from Ahimia and Onion City Dark Web's search engines like google. The anonymity isn't completely verified at the Dark Web. TOR dedicates to it and has intended to offer nameless activities. Here are given effects approximately reporting the quantity of users and wherein place(s) they are. The calculation is primarily based on IP addresses consistent with country codes from where comes the access to them and record numbers in combination form. In this way, indirect are represented the Dark Web customers. The range of users in nameless networks at the Dark Web is some other key element that is resulted. In such networks, customers are calculated through the consumer requests of directories (by TOR metrics) and the relay listing is updated. Indirectly, the variety of users is calculated for the nameless networks.*

Keywords- *dark web, deep web, browser, search engine, website, commerce, hackers, TOR*

INTRODUCTION

As for definition, Dark Web is a part of the net that isn't always visible to search engines like Google and yahoo and requires the usage of an anonym zing browsers and it uses layered encryption Networks. Most of the dark internet contents are unlawful material which usually being used for criminal activities. Dark we may be considered as a number of illicit fabric. A studies achieved by using Daniel Moore and Thomas Rid from King's College in London

located that 57% of Dark Web material is illicit. [1] The websites that we usually use and get entry to, which include this one is at the "clear net". It's not public knowledge, but the clear net sites, such as Face book, Google, YouTube, blogs etc quantity to handiest for around 5% of the total net! The different 90-95% of the net is unhindered and hence is termed as the Deep Web. Also, most of the general public never gets get entry to to the unhindered content material or the Deep web, anything we need, can almost always be discovered on the clear net and without problems too thru search engines like Google and most people are glad with that. [2] The dark internet content material typically exists on private encrypted networks or peer-to-peer configurations. It can most effective be accessed the usage of special software program and decryption equipment consisting of a Tor browser and most of the websites on the Dark Web incorporate fishy content material which need that form of encryption. These web sites cannot be visited the use of engines like Google or traditional browsers as their deal with are encrypted and cannot be traced the usage of traditional methods. The dark web turned into created through the US authorities to allow spies to exchange facts completely anonymously. US navy researchers advanced the technology, known as Tor (The Onion Router) inside the mid-1990s and released it into the general public area for all people to use. The motive became so they could live anonymous - it'd be tougher to distinguish the government's messages among spies if thousands of other people were using the same machine for masses of different things. Tor now hosts more or less 30,000 hidden sites. [3] The Dark Web sites typically use the Tor encryption device to masks their identities because of which they can hold their activities hidden. The device basically functions similar to a VPN and consistently randomizes the host's place to a unique u . S . so it's almost not possible to detect where the user is. Tor-encrypted websites can easily be accessed the usage of a Tor browser. It gives secrecy for both ends – the website and the tourist each. The IP addresses using the browser bounce continuously to random locations whilst getting concealed underneath several layers of encryption. The Dark Web stays incredibly attractive to internet users for a wide variety of reasons. The enshrouded nature and complex methodology required to get admission to this international have effectively made it a secret world, complete of salacious hobby, black markets, sights, and perks restricted to a choose few. [4] The websites may be visited through any consumer in any part of the arena via really inputting the cope with in their Tor browser, however, it is difficult to identify the vicinity or identity of the websites. Depending on how actionable the Dark Web-based pastime is, it is able to be extremely dangerous if the user's identity receives revealed.

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. [5] [6]

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. [5]

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 Hetman and contract killers.

Apart from dark net 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 Black Book, a social network described as the "the Face book of Tor."

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 anonym zing 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 [5].

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 [5]. Currently the most famous dark web search engine is Duck Duck Go. [8]

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. [6] [5] [9]

Dark web sites also use a scrambled naming structure that creates URLs that are often impossible to remember. 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. [6]

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 Alphabet, the dark web's largest source of contraband, sending shudders throughout the network.

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 [2]. 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 [6]. 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 unhindered and still legal, while everything and anything on the dark web is illegal.

DARK WEB IN THE GOVERNMENT,MILITARY AND INTELLIGENCE

Because of the anonymity furnished by way of Tor and other software such as I2P, the Dark Web may be a playground for nefarious actors online. As noted, however, there are a number of areas in which the have a look at and use of the Dark Web may additionally offer benefits. This is authentic not simplest for citizens and companies looking for online privacy, but additionally for certain authorities sectors—specifically the law enforcement, military, and intelligence communities. Anonymity at the Dark Web can be used to protect military command and manage systems within the area for identity and hacking with the aid of adversaries. The army may additionally use the Dark Web to look at the environment in which it's far operating as well as to find out activities that gift an operational chance to troops. For instance, evidence suggests that the Islamic State (IS) and helping groups are looking for to apply the Dark Web's anonymity for sports beyond records sharing, recruitment, and propaganda dissemination, using Bit coin to raise money for their operations. In its struggle against IS, the Department of Defence (DOD) can screen these activities and rent numerous procedures to foil terrorist plots [19]. TOR software can be utilized by the army to behaviour a clandestine or covert pc network operation which include taking down a website or a denial of service assault, or to intercept and inhibit enemy communications. Another use could because navy deception or mental operation, in which the military makes use of the Dark Web to plant disinformation approximately troop actions and targets, for counterintelligence, or to spread data to discredit the insurgents' narrative. These sports can be performed either in assist of an ongoing army operation or on a stand-on my own basis [20]. DOD's Defence Advanced Research Projects Agency (DARPA) is conducting a studies mission, known as Meme, to broaden a brand new seek engine which could uncover styles and relationships in online facts to assist law enforcement and different stakeholders track unlawful activity. Commercial search engines like Google together with Google and Bing use algorithms to give seek consequences by reputation and ranking, and are simplest able to capture about 5% of the Internet [20]. By sweeping websites that are often not noted with the aid of commercial search engines like Google, and capturing hundreds of hidden sites on the Dark Web, the Meme challenge ultimately goals to build a more comprehensive map of Internet content. Specifically, the undertaking is currently developing technologies to "find alerts associated with trafficking in prostitution ads on popular websites" [21]. This is meant to help law enforcement goal their human trafficking investigations [21]. Similar to the military's use of the Dark Web, the Intelligence Community's (IC's) use of it as a supply of open intelligence is not a secret, though many associated information are classified. According to Admiral Mike Rogers, Director of the

National Security Agency (NSA) and Commander of U.S. Cyber Command, they “spend a number of time seeking out people who don't need to be found” [22]. Reportedly, an investigation into the NSA’s XKeyscore program—one in all the programs found out through Edward Snowden’s disclosure of classified statistics— demonstrated that any user trying to down load TOR became automatically fingerprinted electronically, permitting the organization to conceivably discover users who agree with themselves to be untraceable [23]. While particular IC sports related to the Deep Web and Dark Web may additionally be classified, at the least one program related to Intelligence Advanced Research Projects Activity (IARPA) can be related to searching records saved at the Deep Web [24]. Reportedly, traditional gear along with signature-based detection don’t allow researchers to expect cyber threats; as such, officials are responding to in preference to anticipating and mitigating these assaults [25]. The Cyber- assault Automated Unconventional Sensor Environment (CAUSE) program seeks to develop and test “new automated methods that forecast and stumble on cyber- attacks significantly earlier than existing strategies.” [26]. It could use factors consisting of actor behaviour fashions and black market sales to assist forecast and come across cyber events .

CONCLUSION

Nowadays, infinite internet users try to enter the dark net. Some are seeking out something in particular that really can’t be sourced on the ordinary internet, others are clearly curious and excited to go looking what is within the dark web. Some of them are aware how dangerous the dark internet and feature their personal precaution actions to protect themselves, however most of them are recognise nothing and they may be at risk of the harmful of dark internet. Do no longer use dark internet in case you don’t know how to defend yourself. In there, doesn’t mean which you aren't doing crime you are safe, after you enter a whole lot of predators are waiting you to make mistake and flop over your life. Be cautious and remember, do no longer mess with something which you do now not understand. Knowledge yourself first before you cross into dark internet, due to the fact in dark net you are by way of your personal and you need to defend yourself each time, always take your preventive action earlier than you input the dark internet. In Malaysia context, it's far questionable that Malaysian definitely aware of dark internet visibility. The attention approximately the dark net and it risky no longer in clear photo from the authority. Information, analysis, information and observe approximately dark web in Malaysia are still in vague, it's far a incredible possibility and honour if researcher do comprehensive research about the dark net in Malaysia perspective. The collaboration and end result of the studies may be used to prevent and manipulate the usage in addition to awareness to the public with the aid of the authority bodies. The debate surrounding the Dark Web is never over. Online anonymity is a double-edged sword that must be dealt with delicately. As policymakers flow forward, they must display vigilantly the evolution of the Dark Web and ensure that enforcement.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest regarding the publication of this paper.

REFERENCES

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

[2] The Dark Web Links, 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 Ailing 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] Arber S.Bestir,ArsimSusuri,Faculty of Computer Science,University of Prize,"UkshinHoti",Prize,Kosovo.