Implementing Tools For Monitoring And Analysis Of Dark Net Websites

Ajinkya Ghorpade, Shweta B Guja
Computer Science,NBNSSOE

Abstract

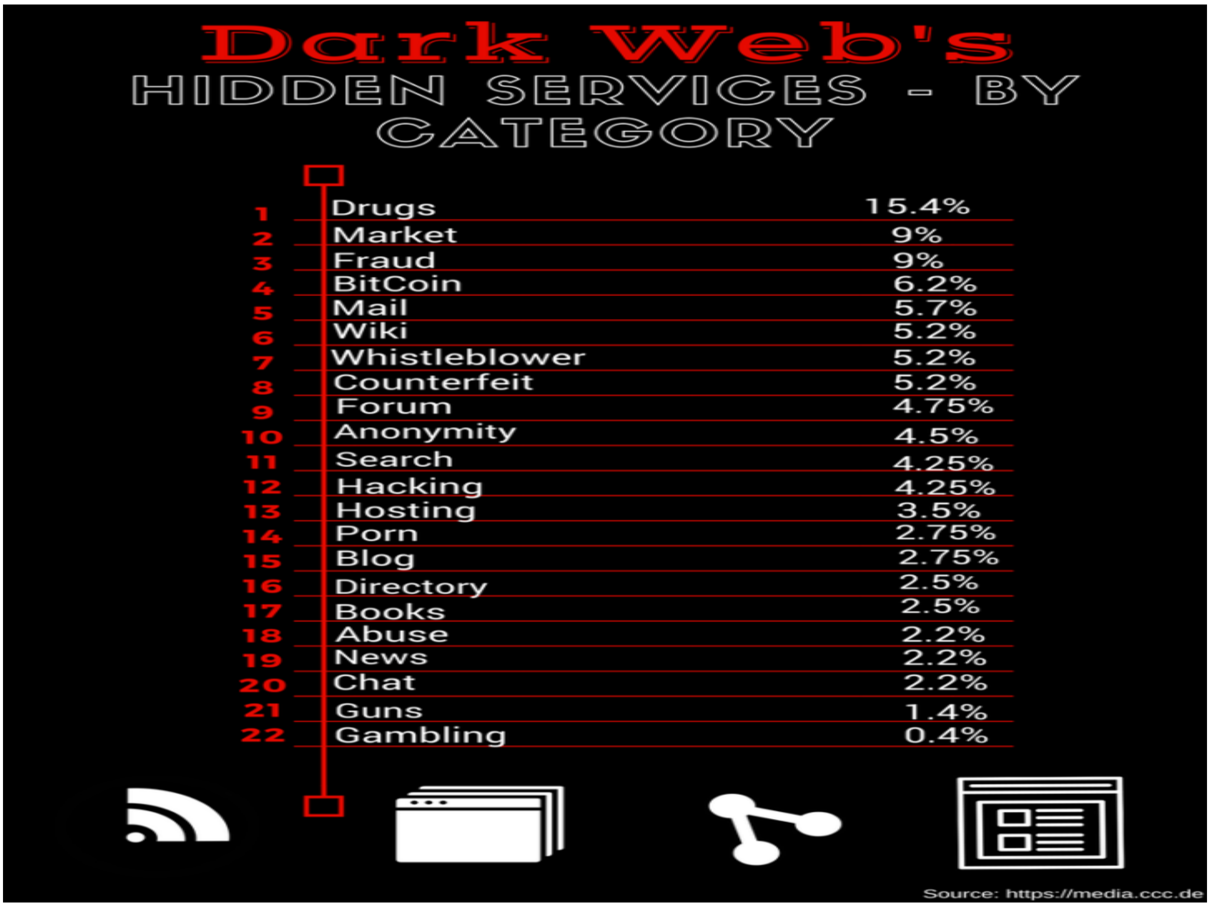
Deep Web is a system of mystery sites that exists on an encoded arrange. The contents of deep web cannot be recorded by standard web indexes. The contents of deep web include web mail, online banking, government resources .The greater part of Deep Web is the Dark Net. The deep web envelops all unindexed destinations that don't appear up when we do an Internet search. The dark net opens the door for black markets like drug dealing, gun supplying, human trafficking and exercises like illicit document sharing and the trading of unlawful merchandise or administrations including taken financial and private information. The dark web can be accessed by use of unspecified browser called Tor . .onion is a pseudo-top-level area have postfix assigning a mysterious concealed assistance reachable by means of the Tor organize .The program directs the page demand through a progression of intermediary servers worked by a large number of volunteer the world over who show ip address untraceable and plain. This research will describe different monitoring tools to trace illegal activities on dark web.

Keywords*—Deep Web, Dark Net, Tor, .Onion, Illegal Activities*

I. INTRODUCTION

The Internet has made information and communication technology very advanced and is accessible to all . If you want any information or want to browse on the web it can be done easily .If you want to talk to anyone, anywhere in the world, you can do it. And all of this is very good at the cost of your computer and bandwidth. We just need a PC or a cell phone and a functioning web association with get to the material. Essentially the web material can be partitioned into three sections the Surface Web, the Deep web and the Dark net.

The pages that can be gotten to through conventional ventures incorporate Google , Firefox , Facebook and so on they fall in the class of the surface web. **Surface web** is a piece of internet that is openly accessible and accessible with web search tools [4]. Only the 5% of contents are available publicly via the surface web [3]. So internet is far bigger than we think . The remaining 95% of the portion is occupied by **Deep Web** and the **Dark Net** [3] **.** The dark web provides support to all form of illegal activities like hacking , human trafficking , weapons and illegal goods , drug dealing and many more. Some of the most popular businesses are listed below. As indicated by measurements , the ordinary browser can get to upto 4 billion sites on the web, and the sites remembered for profound system are a few time more than typical system [4].



Dark Web's
HIDDEN SERVICES - BY CATEGORY

1	Drugs	15.4%
2	Market	9%
3	Fraud	9%
4	BitCoin	6.2%
5	Mail	5.7%
6	Wiki	5.2%
7	Whistleblower	5.2%
8	Counterfeit	5.2%
9	Forum	4.75%
10	Anonymity	4.5%
11	Search	4.25%
12	Hacking	4.25%
13	Hosting	3.5%
14	Porn	2.75%
15	Blog	2.75%
16	Directory	2.5%
17	Books	2.5%
18	Abuse	2.2%
19	News	2.2%
20	Chat	2.2%
21	Guns	1.4%
22	Gambling	0.4%

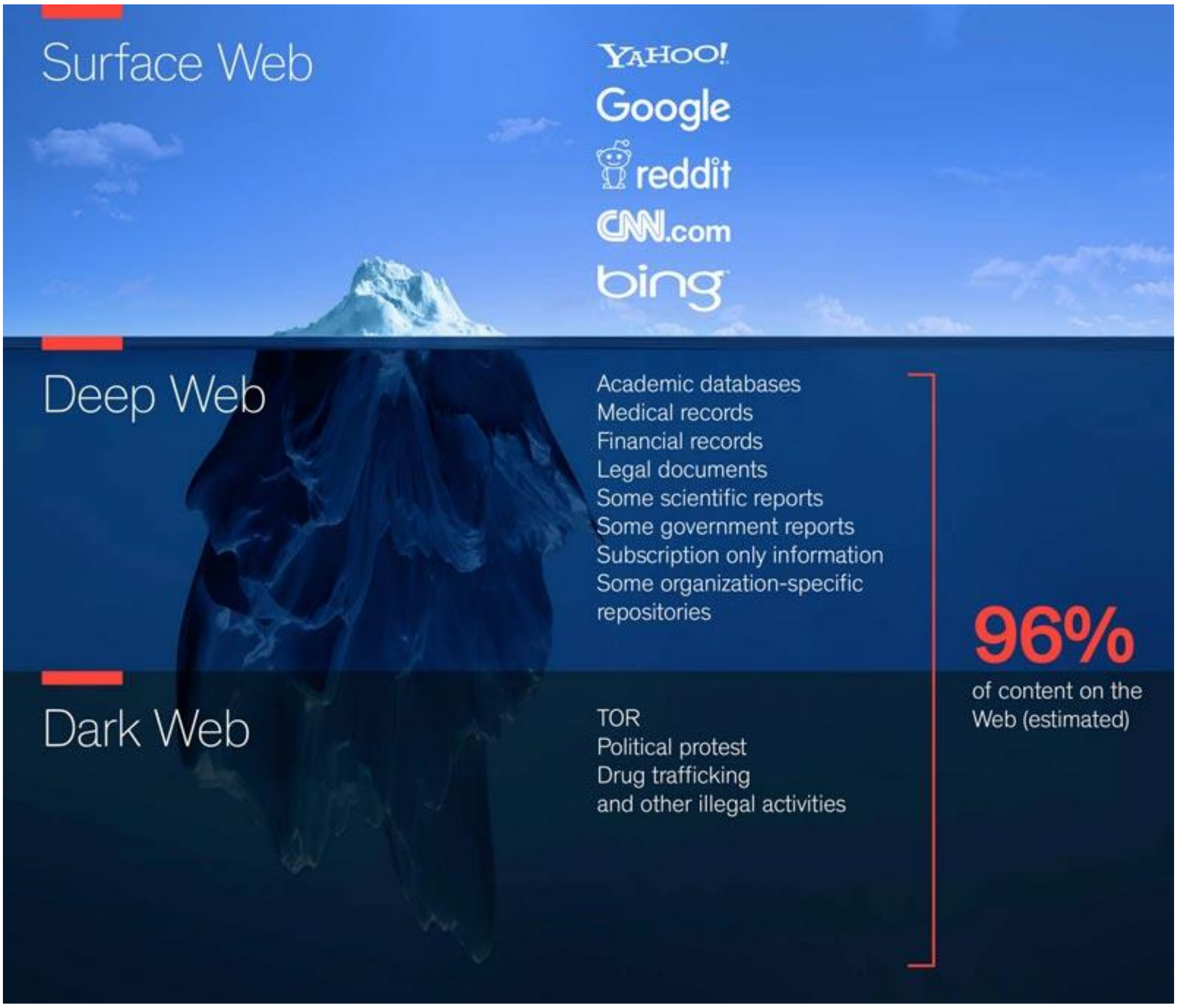
Source: https://media.ccc.de

Percent Wise Illegal activities

II. OVERVIEW

Deep Web

The Deep Web is imperceptible piece of internet whose contents cannot be retrieved by various web crawlers [4]. The contents of Deep Web can be accessed via URLs or direct IP addresses but they may require passwords , encryption or private networks. The deep web is very large as compared to surface web that is hundred times bigger[7] . The data inside deep web is not hidden on purpose .It is just hard for the normal search engine to find it. Numerous web clients are not completely mindful of the crimes occurring over the web .All these activities happen on dark side of the web.

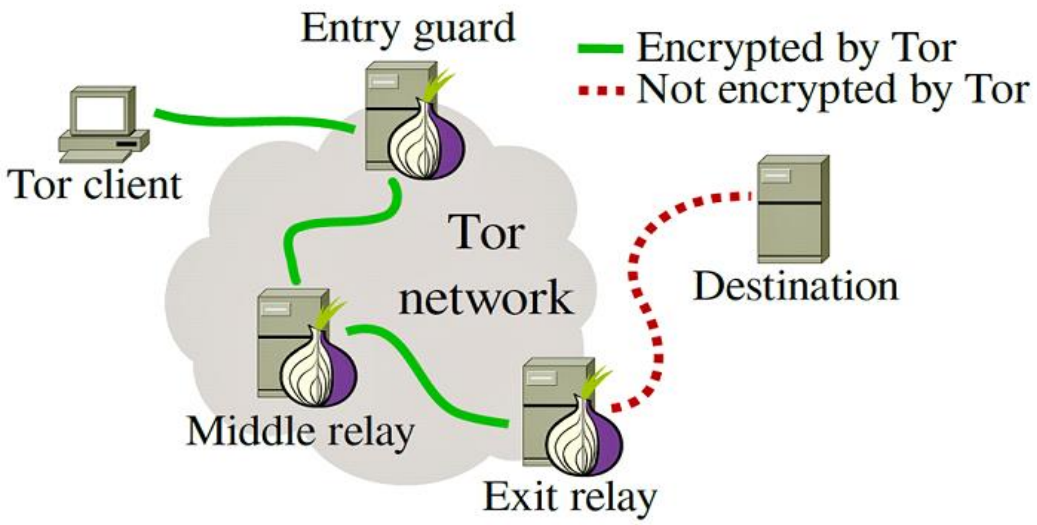


Dark Web

The Dark Web is a piece of World Wide Web whose contents are accessible on various remote systems that utilize Internet however requires different virtual products and setup to get to. The dark web makes up a little piece of the deep web. Some portion of the Web does not appear by web search tools , once in a while the word deep web is utilized in blunder to allude straight forwardly to the dark web. The dark web was really made by the US government in 1990 to trade the data namelessly [1]. The dark web is root to all the criminal operations over the web. Access to the dark system for the most part requires the utilization of explicit devices, for example, TOR, I2P and Freenet [4]. The most well known program is the Tor browser[4].

Tor Browser

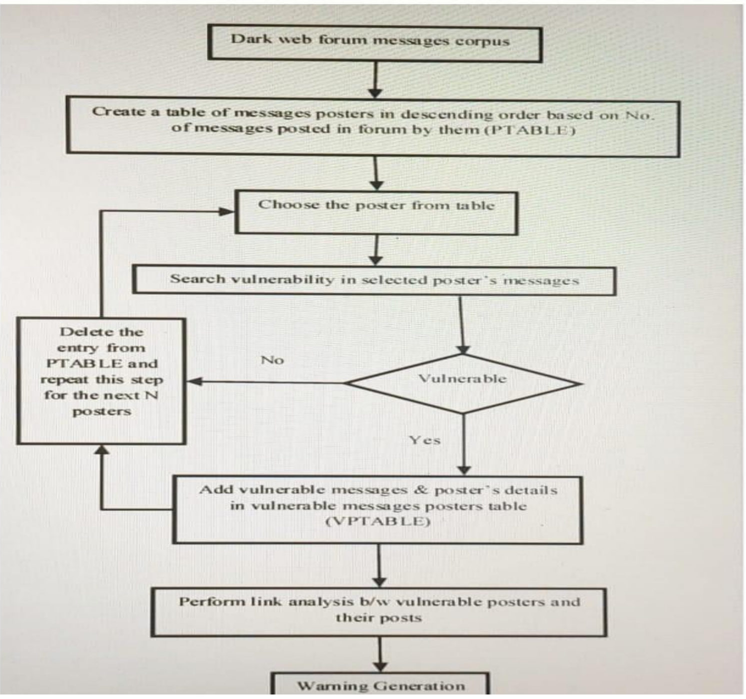
Tor Network is an innovation that is utilized to get to dark web material [4]. Tor is an open source programming for empowering unknown correspondence. The name has been gotten from the abbreviation "The Onion Router". Onion steering is actualized by utilizing encoding in the application layer of communication convention , which is settled like the layers as that of the onion[3].



Working of Onion Router:
Entry Guard: It is the entry point to the tor network. It knows the user IP address but does not know the target IP address [4].
Middle Relay: It is the middle part of tor network and has the responsibility of transferring traffic from ingress router to egress router [4].
Exit Relay: It is located at the border of the tor and is responsible for passing messages to target server [4].

Dark Web Analysis Model

There is a need of an automated system that can perform dark web analysis because manual efforts will take a lot of time to analyse large amounts of the data [5]. In the below model the first step is the data collection from the dark web forum for developing messages corpus[6]. Messages corpus is a collectction of messages and posts posted on the dark web forum. Then a table called PTABLE arranged in ascending order containing the poster name [5]. Then the topmost poster is selected from the table and then vulnerability analysis is performed on the message posted by the poster. If the messages are found to be vulnerable then they are stored in another table called VPTABLE .If the messages are not vulnerable then delete the poster from the PTABLE [5]. A link analysis is performed on top most poster of VPTABLE . And warning is generated .This is how analysis is carried out [5].


Dark web forum messages corpus
Create a table of messages posters in descending order based on No. of messages posted in forum by them (PTABLE)
Choose the poster from table
Search vulnerability in selected poster's messages
Vulnerable
No
Yes
Delete the entry from PTABLE and repeat this step for the next N posters
Add vulnerable messages & poster's details in vulnerable messages posters table (VPTABLE)
Perform link analysis b/w vulnerable posters and their posts
Warning Generation

III. METHODS OF DETECTION

The illegal activities on the dark web include human trafficking ,drug dealing, selling and leaking data related information, hacking illegally, selling weapons and illegal goods, money laundering[1]. So the best method to separate insight from the dark web is to utilize a revelation tool[1]. The apparatus permits organizations to gather dark net danger knowledge data rapidly and without the danger of manual looking through the dark web. These devices are generally utilized for finding .There are numerous devices present in the market both free just as paid. The truth is that no tool is 100 % effective for analysis. Combining of several solutions is the best practice**.**

Echosec Beacon Tool

Beacon Tool is a tool for dark web discovery intelligence. Beacon scans dark web marketplaces, discussion forums, messaging apps, and more so you can detect potential risks to your organization quickly and safely. The tool permits to pull completely recorded information from profound just as dark web sources, for example, onion from their own surface internet browser. Beacon tool is a search engine that can search name, email addresses, social security number through dark web social media , market place and find details of sales and illegal activities. The tool also looks for the websites that mention named person information which is collected for doxing. Doxing targets person in a phishing attack.

Acid Cyber Intelligence

Acid cyber Intelligence is a service that gathers threat intelligence from criminal sites, chat systems , the deep web and the dark net. The data searches are carried out by the web bots. Web bots are internet robots that carry automated tasks assigned to them. The threat intelligence system looks for account credentials , email addresses and its contents , domain name , payment card data . The service provides a account protected dashboard where alerts are displayed when any threat intelligent issue has been identified.

Dark Owl Vison

The Dark Owl Vison is a dark web scanner which indexes the contents of malicious sites all over the world and identify the stolen data. The vison system directly searches company's domain name and email addresses . The searching is completely a automatic process and is updated by repetitive scans and the revelations are made available on dashboard. The information can also be integrated into the applications through the API.

IV. CONCLUSION

Security threats are very frequent in deep as well as dark web . Deep web threat intelligence is very important for the safety of the organizations and also for the safety of the public. In any case, finding and breaking down the dangers securely and proficiently requires a ton of cutting edge apparatuses. So some specified tools for threat intelligence are described in this paper .The tools will help the law enforcements officers and network researchers analyze criminal activities and will also help them to reduce criminal activities.

V. FUTURE SCOPE

The different information analyzing tools can help to trace all the illegal activities and will help to reduce the cyber crime and all illegal activities on the internet.

REFERENCES

1. Alnabulsi, H., & Islam, R. (2018). Identification of Illegal Forum Activities Inside the Dark Net. 2018 International Conference on Machine Learning and Data Engineering (iCMLDE). doi:10.1109/icmlde.2018.00015
2. Schafer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019). BlackWidow: Monitoring the Dark Web for Cyber Security Information. 2019 11th International Conference on Cyber Conflict (CyCon). doi:10.23919/cycon.2019.8756845
3. Hurlburt, G. (2017). Shining Light on the Dark Web. Computer, 50(4), 100–105. doi:10.1109/mc.2017.110
4. YingYang , LinaYang, MeihongYang*, HuanhuanYu, GuichunZhu, ZhenyaChen, LijuanChen (2019). Dark web forum correlation analysis research . 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2019)
5. Sachan, A. (2012). Countering terrorism through dark web analysis. 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12). doi:10.1109/icccnt.2012.6396055
6. Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.
7. Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. International Journal of Rough Sets and Data Analysis, 4(3), 1–16.