JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Empirical study of Dark Web

1Prof. Sunita Totade, 2Dr. V. R. Dhawale, 3Aniket Ramteke, 4Ninad Ramteke , 5 Syed Aamish Iqbal Hussain

HOD, Department of MCA, Vidyabharti Mahavidyalaya, Amravati, Maharashtra, India
2Assist.Prof., K.K. Wagh Institute of Engineering Education and Research, Nashik, India
3,4,5Student, Department of MCA, Vidyabharti Mahavidyalaya, Amravati, Maharashtra, India

ABSTRACT:-

There are basically 3 divisions of internet : surface, deep and dark. The dark web has become Safe isle in the media for being a covert part of the web where all types of illegal activities taken into action. This write-up investigates how the dark web is being operated with an emphasis on cybercrime, and how law enforcement plays the major role of its adversary. The review elaborates these hideouts, sheds light on their history, the activities that they have – including cybercrime, how much attention they receive, and techniques employed by law enforcement in an order to obliterate their course of action . It contains information on private networks and intranets (agencies, institutions, businesses, corporate websites, etc.), web lookup pages or forms searches. Broad Web is also segmented as the Dark Web. Its content are intentionally hidden and are not accessible to standard web browsers & general public. This paper contributes to the area of dark web research by serving as a reference document.

Keywords: dark web, cybercrime, research agenda , cyber crime , law enforcement

INTRODUCTION:-

The term Dark Web and its synonyms such as Darknet, Onionland, the Other Internet, and others have been getting a lot of press these days. Constant reports of identity theft, data theft and state-sponsored hacking have been lingering on headlines on daily basis. Although many people have heard the terms, few actually knows what does it truly means ? The purpose of this article is to explain what it is, what types of content you can find there, who uses it, how to access it, and some of its pros and cons.

So, what is it? The Dark Web is actually a subsection of the Deep Web that consists of networks of all sizes, including large networks run by corporations and small peer-to-peer networks run by individuals. People often use get confused and misinterpretate to mean the same thing. Not everything on the Deep Web is “bad” or illegal. The challenges in these lines of research are varied but are connected to each other. Primarily, the population

being studied is anonymous, cannot be reached by normal ways , and it nurtures their lifestyles or addictions by using illicit details and dark knowledge. Population even take pride in being part of a drug subculture, but from a research perspective, this is not sufficient as the sole reason for sheltering any felons. We require a proper understanding of the complexity of this situation and their subculture is necessary. Using the attributes of public vs private and accountable vs anonymous the internet can be divided into three broad categories .

1) **Surface web**: is publicly accessible because access is unrestricted , hassle free authentication or payment, is indexed by search engines, and is accountable as the stakeholders are identifiable thus subject to law enforcement.

2) **Deep web**: is parts of the internet where public access is prohibited (i.e. private), is not indexed by search engines, and is accountable. Access is restricted due to authentication requirements or because it forms part of an internal network. Accountability here is even robust than on the surface web with respect to authentication requirements.

3) **Dark web**: also known as darknets or hidden services , is a subset of the internet and is not indexed by search engines because it requires the use of special software for access. It has both public and private elements (i.e. accessible publicly or by only those with credentials)correct software is in use.

The key difference between the dark web and surface or deep web lies in the lack of accountability. Users are unidentifiable to the network, or anyone monitoring, and their actions are thus effectively anonymized .Furthermore, the dark web allows for hosting of web services (hidden services) which remain anonymous with regards to their true IP address, and thus location, even to the users who use those web services.

The Dark Web:-

The so-called Dark Web is a part of the Internet, but requires specialized software to access. The well known of these gadget is the Tor (The Onion Router)network, but others such as the Invisible Internet (I2P), also known as “garlic routing”. The main motto behind these technologies is, roughly put to peel layers of routing from the traffic, so that only the previous and next node are known. This makes the web browsing and file transfer much harder, but isn’t impossible, to monitor. Onion routing was originally invented for prudent military communication, but it has since become a small but stable collection of web sites in which anonymity is expected and supported. These sites contain everything from whistleblower data dumps to journalists, spousal abuse victims support groups, and democracy movements’ hidden forums, to drug trading and the sharing of child exploitation images. Even social media companies such as Facebook now provide a Tor-based access to them . The most well-known use of the technology, however, is the establishment of drug trading sites. The now-defunct online marketplaces such as the original Silk Road (2011-2013) and Alpha Bay (2014-2017) are the most famous, but numerous local variations exist. Some of them, like the aforementioned former giants, are so-called crypto markets, where one could use cryptocurrencies such as Bitcoin to mail order narcotics and hormones from sellers advertising on those sites. Others are image boards where people report what they have for sale or what they want to buy, and people then set up face to face (f2f) sales using an instant messaging service such as Wickr

Applications :-

#1 HUMAN TRAFFICKING AND SEX TRACFFICKING:- . About 2.5 million individuals world-wide are trapped in some form of modern-day slavery according to the United Nations Office on Drugs and Crime which is done by illicit dark web activites.

#2 PORNOGRAPHY INDUSTRY:- Victims mostly exploited by pornography industry are women of human trafficking and sex trafficking. Traffickers force victims by fear of assassination for pornography production once male-female sign agreement for accomplishing the acts. The sex trafficker’s records video without the consent of victims and distributes those to interested parties through pornography industry. Traffickers also publishes recordings and photos in their websites. Many web sites related to pornography are hosted in the Dark Web.

#3 ASSASSINS AND MARKETING:- Dark Web is used by criminals to sell their assassin skills. MailOnline, White Wolves and C’thuthlu websites provided advertisement for criminals which mentioned the hiring amount of $10,000 in US and $12,000 in European. For a police officer to high rankling politician this price ranges from 40 thousands to 15 million of hire price. Hidden Wiki and Deep search engines are the most common ways to explore the Deep Web as these contains dozens of links to illicit onion sites.

#4 DRUG TRANSACTION:- Two types of drug markets within the Deep Web are usually found. These include the markets that are dedicated to one specific type of drug such as. heroin. Due to the product expertise and vendor customer relationship these type is much popular. The second type of drug markets is general shop for buyers where all types of illicit products are offered such as weapons, pornography, stolen jewelry, black-market cigarettes and credit cards.

#5 CHILD ABUSE:- Children are using social media and many applications such as Omegle, Ask.fm that hide identity of users for communicating. Pedophiles use the benefit of these applications to interact with the children. Dark Web is massively used by Pedophiles and related criminals for child pornography, sharing photos and pons. Webcam child prostitution has become a growing threat of online child sexual abuse where the victim simply sells his/her live sexual images through Voice-over-IP (VoIP) applications. Using the video streaming feature of VoIP applications live child abuse images are produced and sold for profit.

#6 TERRORISM:- Terrorism and terrorist organizations on the Deep Web are dangerous threat to national security. Terrorist organizations such as al-Qaeda/ISIS and ISIL ISIS have utilized the benefits of Dark Web to fulfill their negative motives and spread propaganda. The Islamic State in Iraq and Syria (ISIS) uses the Dark Web to solicit money to help, support their cause and as a means of passing information throughout the change of command.

#7 MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA:- Applications like Skype and WhatsApp are used by them to send messages across the battlefield and have been able to use small drones to collect real time data to use as propaganda. ISIS recruits by using online magazines with slick production values to communicate their views as well as how to construct weapons for terrorist attacks.

CONCLUSION:-

In this paper, we studied the roles the dark web plays in modern digital society, its establishment of cybercrime and its relationship with law enforcement and society. Conducting review on this topic was challenging as information available and research conducted on the topic is relatively limited due to its 'secretive' and non-identifying nature.

In the debate on privacy versus security, the technology factor is weighing in stronger than before as it becomes not just a matter of legality but of technical capability to monitor and conduct surveillance on people. It is possible that in the future this debate would be over as technology advances to the point where privacy is not at the mercy of governments but in the hands of users and private corporations. The discussion on this topic then no longer remains in the domain of technology but is one that needs an interdisciplinary contemplation by experts in areas of psychology, sociology, law, and others.

REFERENCES:-

Ablon, L., Libicki, M.C., and Golay, A.A. 2014. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Rand Corporation.Ahmad, A. 2010. "Tactics of Attack and Defense in Physical and Digital Environments: An Asymmetric Warfare Approach," Journal of Information Warfare. (9:1), pp. 46-57. Ahmad, A., Webb, J., Desouza, K.C., and Boorman, J. 2019. "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," Computers & Security).

Biryukov, A., and Pustogarov, I. 2015. "Bitcoin over Tor Isn't a Good Idea," Security and Privacy (SP), 2015 IEEE Symposium on: IEEE, pp. 122-134.

A. Oksanen, B.L. Miller, I. Savolainen, A. Sirola, J.Demant, M. Kaakinen, and I. Zych, “Illicit Drug Purchases via Social Media Among American Young People”, in Meiselwitz, G. (ed.), Social Computing and Social Media. Design, Ethics, User Behavior, and Social Network Analysis, Springer,.New York, NY, 2020, pp. 278-288.

D.S. Dolliver and J.L. Kenney, “Characteristics of Drug Vendors on the Tor Network: A Crypto market Comparison”, Victims and Offenders, 11, 2016, pp. 600–620.
O. Enghoff and J. Aldridge, “The Value of Unsolicited Online Data in Drug Policy Research”, International Journal of Drug Policy, 73, 2019, pp. 210-218.
A. Haasio, “What is Disnormative Information?”, Information and Communication Sciences Research, 23(1), 2019, pp. 9-16. M.C. Van Hout and T. Bingham, “‘Silk Road’, the Virtual Drug Marketplace: A Single Case Study of User Experiences”, International Journal of Drug Policy, 24, 2013, pp. 385–391. M.C. Van Hout and T. Bingham, “‘Surfing the Silk Road’: A Study of Users’ Experiences”, International Journal of Drug Policy, 24, 2013, pp. 524–529.