Exploring Anonymous Depths of Invisible Web and the Digi-Underworld

Iflah Naseem
CSE
IET-DAVV
Indore, MP

Ashirr K. Kashyap
CSE
IET-DAVV
Indore, MP

Dheeraj Mandloi, PhD
Faculty of Chemistry
IET-DAVV
Indore, MP

ABSTRACT

Internet and World Wide Web are the basic necessities of everyone these days, may it be e-commerce, or social networking or transferring files and information. With advancement in technology the World Wide Web is growing and bringing out new aspects.

Since it is of utmost importance in commercial world today, it is known by people all over the globe. People use it daily and it has become a path and parcel of lives. Though people explore it daily, but most of them don’t have slightest idea of the actual depths of the web. Most of the internet using population surf the surface web and have no idea about the hidden side of the web, which ironically is about hundred times larger than the web people mostly use.

Along with ever growing techniques, the surface web is growing daily in a fast decent pace but the deep web is growing exponentially. The deep web is so large that it is hard to estimate its size.

Deep Net is usually known for its privacy ensuring facility and preciseness. Unlike surface web, it is more efficient in giving results for browsing.

The Deep Net further has various aspects, including Dark Web, which now acts as a platform for smuggling and more malicious activities, taking advantage of the privacy provided in this means.

With Deep Net and Dark Net coming into play, dark markets have also been established, which remain hidden and never come in frontline. In their concealed form, they carries out their business effectively. The transactions are made here using digitalized currency called Bitcoins.

General Terms

Deep Web, Dark Net, Surface Web, Clear Net

Keywords

Bitcoins, the Tor Project, Hidden Wiki, Silk Road

1. INTRODUCTION

The Deep Web, hidden web or invisible web is a subset of the World Wide Web which remains hidden due to many reasons and is not indexed by search engines.

Search engines use software called as crawlers which are ineffective in finding information accessible in enormous databases that can only be searched through dynamic queries or website pages which are not connected to by other pages or scripted content or Private Web or information hosted on anonymizing networks [1].We cannot precisely estimate the size of deep web but it is said that it is approximately about 100 times larger than the surface web because it mainly contains databases. A small segment of the deep web comprises of Dark Net which can only be accessed by special software such as TOR browser, I2P, freenet software etc. All these software provide privacy and provide a secure channel where the client and server can communicate without being concerned of their identities. The TOR network is open software and a free network that protects its users against any form of network surveillance and monitoring activities that invades personal freedom and privacy or business activities, and traffic analysis.

Tor protects its user’s online activities by first encrypting and then hopping communications around a vast distributed network of relays run by volunteer servers all around the world. By this technique it prevents malignant people from intercepting the internet connection and monitoring which sites you visit, and it prevents the sites you visit from learning from what are you browsing.

Although the TOR network is not completely secure but it enables a web which is extremely hard to track and monitor anyone’s activities.

The dark web facilitates the existence of dark markets, where illegal trading is carried out. It comprises of selling and buying of stuff which cannot be sold in a free market on surface web. It provides a platform to smuggling and trade of other illegal products comprising drugs, arms and ammunitions.

The ecommerce of this black market is braced with digitalized currency called Bitcoins. It makes the transactions possible in its hidden form. Bitcoin is primary key for transactions of black market.

The difference between Surface Web and Deep Web is described in section 2, then the meaning of Dark Net is described in detail in sub-section 2.1.The Tor Browser and other anonymizing software are depicted on sub-section 2.2. Working and creation of Bitcoins is explained in sub-section 2.3.Variety of illegal activities happening on the Dark Net are discussed in sub-section 2.4.The reaction of law enforcing agencies is shown in sub-section 2.5. The future of deep web in section 3. Finally, the paper is concluded in section 4.

2. SURFACE WEB AND DEEP WEB

The World Wide Web could be compared to an ice berg where the part below the surface is much greater than the one lies above.

World Wide Web is composed of mainly two parts – Deep Web and Surface Web.

Surface Web or Clear Net makes about 4% of the World Wide Web. It comprises of those parts of the World Wide Web which are indexed by a search engine and anyone can easily access it. Google, in spite being the largest search engine has indexed only 6%-7% of the total web.

The Deep Web, the subset which is not directly available makes about 96% of the total World Wide Web. It consists of those parts which are not indexed or accessible by any standard search engine.

Google and other search engines make use of web crawl or spider web pages [2]. This facilitates of the process of jumping from one hyperlink to another along with gathering relevant information and maintaining an index of the same. Also some authors index their websites to search engines so that their websites have accessibility in search results of other search engines.

Referring to figure 1 the deep web is composed of information such as online banking, sites that require registration and login, limited access content, Non-HTML content, and scripted content, content that may only be accessed through specific software and much more [3]. It is impossible to measure and hard to estimate the size of the deep web because majority of the information is concealed inside databases. The content of deep web is highly apt to all information need and domain. It customarily dispenses the precise results.

Also deep web is comparatively narrower to the surface web, since it is more restricted. Deep web also face way more traffic than the surface web, and is quite highly and complexly linked too. It provides relevant and precise information [4].

Contents of deep web cannot be indexed completely because majority of its content constitute of password protect or has limited access or can be accessed through a particular software only [5].

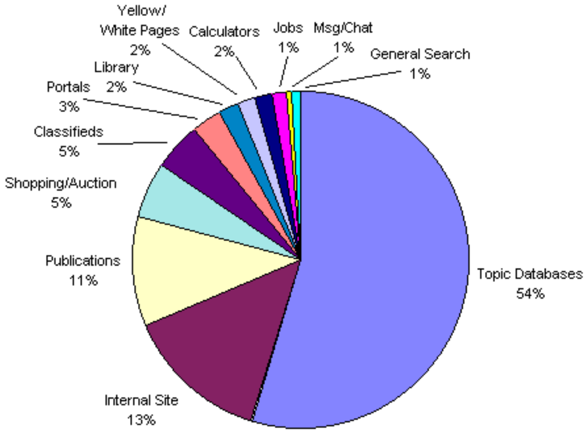

Figure 1. Distribution of Deep Web Sites by Content Type

2.1 Anonymous Deep Web –The Dark Net

The Dark Net or the Dark Web is a subset of the Deep Web. It is the anonymous part of the deep web which can only be accessed by using anonymity software such as “The TOR Browser” or specific authorization and configuration. It makes use of unauthorized means of communication and ports. This part of network usually follows peer to peer or friend to friend network topology.

Due to its anonymous nature it has evoked a lot of illegal businesses and malicious activities. This includes trading of unlicensed objects illegally, also releasing of data or information whose copyright lies with some organization [6].

The much darker side Dark Net consists of underground and infamous subcultures such as social media racists, self-harm communities, Darknet drug markets, crypto anarchists, hackers and Trans humanists. All of these are too controversial to exist on surface web, so they lie within, moreover in an autonomous form [7].

Although the dark net is mainly used for illegal activities, it also has some good uses such as it can be used a whistle blowing platform that is an open platform to report illegal deeds and many journalists use it to expose the wrong doings of big organizations which they would be never able to do in via surface web. One such website is Wiki-Leaks which was taken off the Clear Net because it leaked very sensitive information about some governments but WikiLeaks is still present on the Dark Net and is still is in completely functional mode and is still being used to expose secrets and other sensitive information[8].

2.2 The Tor Browser-Gateway for the Dark Net

TOR stands for The Onion Router. The Tor Browser is an extension of Mozilla Firefox. It protects the privacy of its users, be anonymous and improve their security by jumping through various distributed networks and connecting via a group of virtual tunnels instead of making a straight connection. Both Clear Net and the Dark Net can be accessed by using Tor browser [9].

Unlike the links of a clear net website the dark net websites end in onion (dot onion) domain suffix which is only accessible through a Tor network. In an onion network, messages are wrapped in layers of encryption, similar to the layers of an onion.

Links of the dark net can easily be found on “hidden wiki” which is a clear net website and also exists on dark net which maintains database of quite a few darknet links.

Usually the search engines monitor the user and their activities via cookies, which are small chunks of data which is stored in user’s web browser and this information is then used to feed advertisements. These cookies works in accordance with the search made or sites visited and hence let the sites pop advertisement of similar interest.

2.2.1 TOR

The tor network can be used for anonymously browsing the web which prevents the search engines and local ISPs to monitor user activities. Hence the role of cookies is totally discarded here, eliminating the pop up advertisements.

TOR was created to secure communications and escape censorship as a technique to guarantee free speech. But now is used to carry out a huge variety of malicious activities too.

2.2.2 I2P

I2P stands for Invisible Internet Project. I2P network is an anonymous overlay network. Its main aim is to protect communication from surveillance and monitoring by ISP’s and search engines. I2P’s exclusive goal is to provide a way for users to host services.

It is free open source software which facilitates chatting, blogging and web surfing. It make use of crypto currency for transactions.

2.2.3 Freenet

Freenet is software which lets people secretly share files, view and publish “freesites” without any fear of censorship and it is very strenuous to detect when used in darknet mode. It also supports microblogging. It is also a peer to peer network. It differs in the user interaction way, it separates the under lying layers of protocol and networks from the user interaction interface.

All the communications are encrypted, in a similar manner how it is done in TOR and freenet which makes them really hard to track.

As compared to I2P and TOR, Freenet offers less extensibility in terms of hosting services, being limited to serving only static content, but sill provides access to huge variety of content.

It works as a large version of cache, since instead of simply exchanging data like peer to peer network; it stores and then transfer data. Though being massive platform, its scalability is appreciably good, since its performance never deteriorate with the expansion of network.

Freenet cannot be a suitable platform to host dark marketplaces or exchange information related to illegal activities [10].

2.3 Bitcoins –Currency of the Dark Net

A Bitcoin is unit of digital currency which is utilized in dark online markets also referred as crypto markets.

On buying a product or employing a service the customer pays to the site escrow in form of Bitcoins, after the delivery of product or completion of service, the vendor claims payment from website and the customer leaves the feedback against the vendor's account. This reduces the possibility of fraud to a great extent [11].

Just as a bank needs employees in a similar manner people or workers are needed to carry out computations and calculations about these transactions of crypto market these people are known as Bitcoin miners.

After every transaction the record is publically recorded on a distributed database. Miners verify the transaction in the database after a certain amount of transactions have been verified by a minor that miner receives newly minted Bitcoins for his work. This is how new Bitcoins are brought into circulation [12].

Miners execute Bitcoin mining through mining software like Cgminer, Bfgminer, Bitminter, Btcminer, Poclbm, Diablominer etc.

Although mining can be performed on any computer but special hardware is also available which enhances the mining process by a great factor. Bitcoin ASIC (Application Specific integrated Circuits) chips are used which generally can only be used for Bitcoin mining some chips are Antminer S5, Avalon6, SP20 Jackson.

Currently about 12 million Bitcoins are in circulation and the creation is capped at 21 million.

2.4 Malicious Activities on the Dark Net

Due to its anonymous nature, the Dark Net has attracted lots of illegal activities such as Hacking services, hiring contract killers, selling of narcotics, exchange of fake documents such as pass ports and credit cards, illegal arms, unlicensed pharmaceuticals, steroids and ammunitions etc.

Trading on dark market let its users to evade taxes and other duties too. It also provides much entailed privacy to its users.

One such website was "Silk Road" also known as "The Amazon of illegal drugs" which was an online black market launched on February 2011.It was mainly known for selling drugs, stimulants and psychedelics. Silk Road was shut down by the FBI (Foreign Bureau of Investigation) and its owner was arrested but still the website is functional under some other means and link [13].

Many terrorists use TOR as a safe communication platform as their communication cannot be tracked or intercepted by the FBI or other anti-terrorism agencies. They also use TOR as a means to spread propaganda and terrify creating turmoil and terror anonymously.

Credit cards, pass ports, duplicate identity cards and other counterfeit documents can be bought via these online black markets.

Even the Twitter followers can be bought on the dark net, for about 25$ user can buy about 2500 followers.

Weapons, arms and ammunition can be purchased on illegal weapon trading websites [14].

2.5 Law enforcing the Dark Net

To stop these illegal activities the FBI and other law enforcing agencies have taken various steps and Silk Road was shut down by the FBI October 2013. Silk Road 2.0 was shut down by FBI and Europol on 6 November 2014 .Silk Road 3.0 is online.

Many white-hat hackers have been employed by the FBI who make numerous attempts tracking illegal activities and people associated with them [15].

The law enforcing agencies are developing new methods and becoming more technologically savvy to apprehend these criminals.

Agencies try to follow the money trail and track the Bitcoin transactions.

UK has set up a unit to tackle Dark Web criminals who use the country's mass surveillance capabilities to track them down.

2.6The future of deep web

The deep web tends to become way more secure than what it is in present time, ameliorating the covertness of darknet and discovering new ways to become more anonymous.

The dark markets will become well built in near future. There will be a boost of absolutely decentralized markets that depend on Bitcoin's block chain technology. Implementation of developed markets shearing even minute breakdown is expected.

Gauging reputation will become easier in coming time. It has become crucial in the situation of high obscurity to be able to assure faith and reputation, among vendors and consumers without having to depend on a foreign authority like banking organizations as in canonical e-commerce.

Bitcoins will emerge as tough to track currency. Crypto-currencies go conjointly with Deep Web and its markets. Hence we'll identify contemporary and advanced techniques to compose Bitcoins even less traceable as compared to present form. Also, malware could take an edge in the block chain technology.

Count of users of deep web will boost in near future, since with rise in technology, awareness will also grow among the users of web, soon there will be a huge increase in number of users of darknet and Deep Web.

3. CONCLUSION

As we know that the deep web is expanding exponentially, so is the darknet which is giving way to enormous illegal activities providing platform, which is forcing the law enforcing agencies to use new unorthodox methods to track these technologically savvy criminals.

These software are frequently used by whistleblowers, journalists, military and even terrorist organizations to access a secure channel for communication.

Virtual currency which is used in dark market transactions is termed as Bitcoins. It is a very secure and flawless way of carrying out e-business.

No one can be completely anonymous on internet but software such as TOR, freenet and I2P make it extremely strenuous to track its clients. This gives them freedom from censorship, privacy, a secure channel to communicate.

The future of Deep Web includes much more secured and improvised darknet, more power and well established market places for darknet, gauging information will become easier, tracking down of Bitcoins that is the currency of dark markets will become harder and moreover, with increase in awareness among people will result in more users of darknet and simultaneous expansion of the same.

4. ACKNOWLEDGMENTS

We have tried our best to present this research as simple as possible using basic terms that we hope will be comprehended by the widest spectrum of researchers, analysts and students for further studies.

We have completed this study under the able guidance and supervision of Dr. Dheeraj Mandloi .We would like to thank esteemed scholarly, assistance and knowledge we have received from him towards fruitful and timely completion of this research paper.

We would also like to thank our Institute of Engineering and Technology and faculties who provided us with necessary guidance, provided us insight and support.

5. REFERENCES

[1] Christopher.Web CrawlingThe Stanford University InfolabFoundations And Trendsr In Information Retrieval Vol 4 .Web Crawling.

[2] Sherman, C., & Price G. (2001).. Medford, NJ: CyberAge Books, Information Today. The invisible web: Uncovering information sources search engines can'tsee.

[3] Bergman, M. (2001).Presented by Mat Kelly,CS895 – Web-based Information Retrieval,Old Dominion University,Septmber27, 2011.The deep web: Surfacing hidden value.

[4] Marcus P. Zillman.Virtual Private library, January 1, 2016.Deep Web Research and Discovery Resources.

[5] Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler .Trend Micro,ATrendLabs .Research paper Below The Surface: Exploring The Deep Web.

[6] Daniel Sui,JamesCaverlee,DakotaRudesill.A Wilson CenterPublication The Deep Web and The DarkNet:A Look Inside The Internet's Massive Black Box.

[7] Peter Biddle ,Paul England,MarcusPeinado ,Bryan Willman.Microsoft Corporation, Redmond, WA, 98052, USA. Digital Rights Management(page 155-156).

[8] Kristin Finklea.Congressional Research Service.July 7,2015.DarkWeb.

[9] Vincenzo Ciancaglini. (10 March 2015). TrendLabsSecurityIntelligenceBlog. The Deep Web: Shutdowns, New Sites, New Tools.

[10] Steven R Gruchawka..November 2005 .Using the Deep Web:A How-To Guide for IT Professionals.

[11] Dean, Matt. 2014. Fox Business,December 18. Digital Currencies Fueling Crimeon the Dark Side of the Internet.

[12] Jesse Hamilton and Olga Kharif, Aug. 26, 2013 Bloomberg.Bitcoin Foundation Meets With U.S. Regulators, Law Enforcement.

[13] Regional Organized Crie Information CentreSpecial Research Report .2013.Penetrating The Darknet ROCIC.

[14] Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler.Trend Micro,ATrendLabs Research paper. Deep Web and Cyber Crime.

[15] Michael Chertoff and Tobby Simon .Global Commission on Internet Governance paper series no.6-februrary 2015.The Impact of the Dark Web on Internet Governance and Cyber Security.