DARK WEB-DO HEALTHY THINGS TO HUMAN OR NOT!

P. Ramesh[1], G. Pavan Babu[2], J. Sandeep Raj[3], Y. Udaya Kumar[4]

[1.2.3.4]III MCA, SITAMS, Chittoor, A.P.

Abstract : Nowadays providing solutions to information Security becoming challenging task, as many counter solutions are coming in to the market which gives counter solution to the existing solutions given for the security. In this concern, Dark Web is a WWW web content, which is misused by many unwanted group of people, though they have their own merits of usage. In this paper, it is addressed about the procedure behind dark web, its merits and demerits of using this dark web.

Keyword: Dark Web, Deep Web, Surface Web

I. INTRODUCTION

In computer security terms like “Deep Web” and “Dark Web” are often leads to confusion The Internet: This is the easy one. It’s the common Internet everyone uses to read news, visit Facebook, and shop. Just consider this the “regular “Internet.

The Deep Web

The deep web is a subset of the Internet that is not indexed by the major search engines. This means that you have to visit those places directly instead of being able to search for them. So, there aren’t directions to get there, but they’re waiting if you have an address. The Deep Web is largely there simply because the Internet is too large for search engines to cover completely. So, the Deep Web is the long tail of what’s left out.

The Dark Web

The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but require specific software, configurations or authorization to access [1]. The dark web forms a small part of the deep web, the part of the Web not indexed by search engines, although sometimes the term "deep web" is mistakenly used to refer specifically to the darkweb.

SurfaceWeb

- 4% of WWW content
- Also, known as the ‘Visible Web’, it is content that can be found usingsearch engines such as Google or Yahoo [3]. It is under constant surveillance by the government.

Dark Web

- 96% of WWW content
- Also, known as the ‘Invisible Web’, it is the content that cannot be indexed by search engines. And it is hard to keep track of.
- The Dark Web is estimated to be at least 500x the size of the Surface Web.

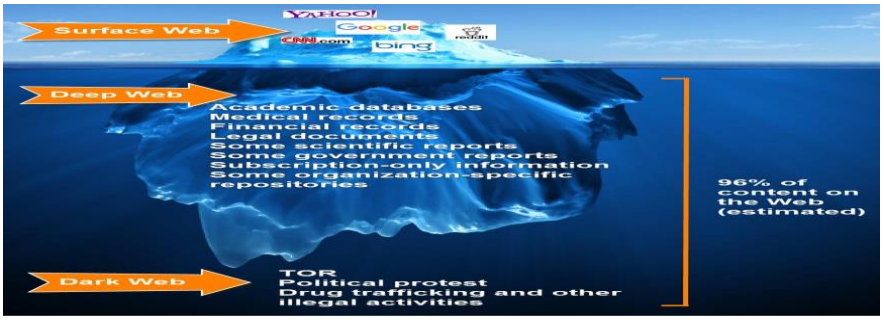

Figure 1: Comparison of Different Web

II. ABOUT

The Dark Web (also called Darknet) is a subset of the Deep Web that is not only not indexed, but that also requires something special to be able to access it, e.g., specific proxying software or authentication to gain access [1]. The Dark Web often sits on top of additional sub-networks, such as TOR, I2P, and Freenet, and is often associated with criminal activity of various degrees, including buying and selling drugs, pornography, gambling, etc.

While the Dark Web is definitely used for nefarious purposes more than the standard Internet or the Deep Web, there are many legitimate uses for the Dark Web as well. Legitimate uses include things like using Tor to anonymize reports of domestic abuse, government oppression, and other crimes that have serious consequences for those calling out the issues.
Common Dark Web resource types are media distribution, with emphasis on specialized and particular interests, and exchanges where you can purchase illegal goods or services [1]. These types of sites frequently require that one contribute before using, which both keeps the resource alive with new content and also helps assure (for illegal content sites) that everyone there shares a bond of mutual guilt that helps reduce the chances that anyone will report the site to the authorities.

III. ACCESS MECHANISM OF DARK WEB

What you want to access are sites using the Tor Hidden Service Protocol. It works over regular Tor (anonymity network), but instead of having your traffic routed from your computer and through an onion-like layer of servers, it stays within the Tor network. You won't know exactly what system you're accessing unless they tell you [1], and they won't know who you are unless they do - or unless one of you is careless.

Step 1: Go and get yourself a good VPN (Virtual Private Network), use it ALL of the time, no matter if you are on TOR or not. This site here reviews the best VPN's for use with TOR.

- ➢ You should be taking your anonymity and security very seriously if you are visiting the Dark Web, especially if you are viewing any Darknet Markets.
- ➢ DonotfoolyourselfandthinkthattheISP's(InternetServiceProviders)andLawEnforcement are not trying to track those who use Tor to access the Dark Web, they are, and they are good at it so don't make it easy forthem.
- ➢ What's even better is that the VPN will give you a fake IP address, in another country if you like, so even if Tor is compromised then the trace just leads back to somewhere else that can't be linked to you.
- ➢ The other benefit of using a VPN is to prevent hackers stealing your identity and or personal files and photos from your computer.
- ➢ You need to use a good VPN that keeps NO LOGS, fast performance, preferably accepts bitcoin as payment, has a kill switch for DNS leaks, and is compatible with TOR.
- ➢ Then install your VPN, if you buy one of the better VPN's then it is usually just a one click install and one or two clicks to turn it on.

Step 2: You can't access the deep web just using a common browser like Internet Explorer or Google Chrome. To get dark web access you will need to download the dark web browser called TOR browser bundle. Only get it from the official TOR website, never download it from anywhere else!

- ➢ Now close all of your browsing windows and all apps connecting to the internet like Google Drive, Skype, OneDrive, iCloud etc.
- ➢ Then open your VPN app and connect to another location other than where you are at, make sure to use the OpenVPN protocol as it is the most secure.
- ➢ Open up your normal favorite browser and then download TOR
- ➢ TOR Official Website: https://www.torproject.org/download/download.html

Step 3: Install the TOR browser bundle on your PC or Mac. When the download is complete, double-click the downloaded file, choose the destination folder (the folder where you want to extract tor browser), and choose extract.

Step 4: Start TOR Browser. Open the folder where you extracted TOR browser and double-click "Start Tor Browser". The TOR start page will open in a browser window (it's actually a portable version of FireFox striped down).

- ➢ From here, you now have a good level of anonymity and security and you are able to gainaccess to .onion websites through your dark web browser.

Step 5: DO NOT change the TOR browser window size unless you like living dangerously. The FEDS have programs that can match identities on random things such and matching time online and other things with the browser window size, I shit you not. If you don't change the size, then it is the same as most other people.

Step 6: Please remember that TOR isn't necessarily 100% anonymous, you should turn off JavaScript within the dark web browser settings to help.

Step 7: Disconnect your webcam or block the camera with some black tape. Hackers and governments have ways of getting into your computer and turning on the video and cameras.

- ➢ You can have intimate images of you be used as blackmail or extortion, or even worse, used by the feds.

Step 8: Disconnect your microphone or cover it with tape to muffle it good. The same goes for the microphone as the camera, the last thing you want is to be recorded saying incriminating things at home. It doesn't even have to be while on the dark web.

Step 9: NEVER use your real name, photos, email, or even password that you have used before on the dark web. This is the fastest way to be tracked. Use an anonymous email account and aliases that have nothing to do with you that you have never used before.

Step 10: If you are using TOR on the dark web for anything other than looking at cute pictures of kittens, you should think seriously about your privacy and security. Jolly Roger has put together a comprehensive guide on how to stay safe on the deep web.

IV. ADVANTAGES

For example, let's say you're looking for a really rare movie (e.g. Abel Ferrara's The Addiction) that was never released on DVD. You've searched high and low for this movie on the Clearnet, and haven't found it. However, it's highly possible that someone on the dark web may have it. You can also find certain technology (e.g. the iPhone 6s Plus) cheaper than you could find it on the Clearnet [2]. The downside may be that either of these were illegally copied or stolen, which is always a risk you take on the dark web. That's why exploring it takes time and experience.

Beyond that, if you live in a country that has an oppressive regime (e.g. North Korea), and want to have more freedom, the dark web can help you establish that. Some people write blogs about their experiences in such countries on the dark web, and while it's possible that they could be traced , it's far less likely, if they take the right precautions [2]. Journalists and whistleblowers also use it sometimes, for similar reasons.

There are also quite a few special-interest communities and subcultures on there (even though these exist on the clearnet too). Many are for hackers, writers, and people concerned about censorship. So, the *major* drawbacks of the dark web is a sense of community and freedom that some don't feel on the surface web.

4.1 Anonymity

To be completely honest, that one is a double-edged sword. Anonymity results in freedom, which sounds perfect. Sadly it is also the honey that attracts all the criminal activity that gives the deep web such a bad name.

To appreciate the anonymity that browsers such as Tor (there are others, but they are not as user-friendly) we need to realize that our web actions leave traces of ourselves, a massive amount of personal that shapes what is known as our digital identity. Both companies and governments are extremely interested in monitoring our behavior, and many users prefer to hide their identities to avoid political, economic or social harassment.

To guarantees that the user IP address cannot be tracked (to add an extra layer of security it would be recommendable to log into Tor via a VPN network). It is not that anonymity is not a crime; it is actually a legally recognized right.

4.2 Freedom of speech

That would be a direct consequence of anonymity. The right to freely express your opinion on any topic without fearing persecution that most western countries take for granted (although with these matters, you never really know what might happen) is almost a utopia in certain parts of the world.
Overcoming censorship is another really positive feature that deepnet has allowed, which directly links us to our third benefit.

4.3 Political Activism

The deep web has result in a speaker for noble causes. Oppressive governments are a crude reality in the 21st century. Information is a very powerful weapon to this kind of regimes, and its citizen's movements on the World Wide Web are strictly monitored to avoid the spread of revolutionary ideas. Blocking websites, especially the ones related to social media, is a common measure in oppressive environments. It is in this context that browsers such as Tor appear as a solution to enable a safe communication line not only in a national level, it also allows international denounce certain situations. The deep web has had a major role in recent historical events such as the Arab spring.

4.4 Knowledge

The deep web stores the largest virtual libraries you could possibly imagine. It is a great space for researchers, students and teachers, since what they can find in the deepnet will more probably not be available from standard search engines. Scientific findings that have not made public and could influence health and social beliefs of large populations can be found in the deepest of the web waters. Literature from all ways of thinking that you will not find in the book storefronts (pro-suicide, anti-moralism…)are also stored in the deep web.

4.5 Amazing individuals

How we act with the resources we have access to concerns our individual responsibilities and judgment. Certain person in what could be called "the deep web community" is dedicating both time and effort to help other altruistically. From doctors giving professional advice on "The silk road" (drug's eBay) to individuals who are investigating to expose who is behind the major crimes sites there is a whole movement trying to make the deep web a better place.

V. DISADVANTAGES

Since there's more content to analyze, Deep Web search engines tend to be slower than standard search engines. Searching the Deep Web also requires a more precise search string. Deep Web searches should be reserved for serious, painstaking research, not for simple questions and basic Web surfing. Deep Web searches may also return sensitive personal information from normally restricted databases, creating ethical dilemmas and leaving individuals susceptible to fraud and identity theft.

Everything on the deep web is completely untraceable and it's only a matter of time before criminals take advantage of it. To put it simply, the deep web has become a corrupted hub of criminal activity. The transfer of drugs, illegal weapons and the hiring of contract killers is an almost daily occurrence on this medium.

Illegal bidding market places similar to E-bay have been set up on the deep web to sell these illegal goods and, no matter how hard they try; there is nothing the law can do to stop it. These illegal market places are extremely efficient and even boast a user-friendly interface and search bar to help criminals save time in locating their illegal goods. The currency used in these marketplaces is the cyber currency Bitcoin, which only adds to the impossibility of the transfers and guilty parties being traced.

The deep web has been around for many years however, it was not until October 2013 that the general public really began to become aware of it. This was due to the primary deep web market place, 'The Silk Road', being shut down by the FBI, with its creator and host being arrested. The creator was caught after he tried to hire a hit man through the site who was actually an undercover FBI agent.

Although this was a major breakthrough for the authorities, many other illegal market places have since sprung up to take The Silk Road's place, meaning that the law is now back at square one in terms of preventing illegal activity on the deep web. The deep web may sound like a dangerous place to venture and, to be brutally honest; the everyday person can live in complete ignorance of it and still be perfectly content. However, it does have some (legal) practical uses.

CONCLUSIONS

Though many security systems with different technology are existing in the market, the usage of that technology and security mechanism must be followed in controlled way by all users by taking the positive notion of the same in which everyone can enjoy the essence of available systems.

REFERENCES

[1] M. Chertoff, T. Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Centre for Int'l Governance Innovation and Chatham House, Feb. 2015
[2] "Cybersecurity Experts Uncover Dormant Botnet of 350000 Twitter Accounts", *MIT Technology Rev.*, Jan. 2017.
[3] M.K. Bergman, "The Deep Web: Surfacing Hidden Value", *J. Electronic Publishing*, vol. 7, no. 1, 2001.