Dhole Patil College of Engineering, Pune
Department Of computer Engineering

Monograph on

DARK WEB

Submitted By-

1) Prof.Varsha R.Dange
2) Kaushal Makan(SE COMP)
3) Manish Jha(SE COMP)
CONTENTS:

1. Introduction
2. What is Dark Web?
3. How to access it?
4. Applications
5. Advantages
6. Disadvantages
7. Conclusion
INTRODUCTION:

If you’re into computer security at all you may have heard of terms like “Deep Web” and “Dark Web”. The terms can be confusing so here are the basics:

- **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. 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 dark web.

- **Surface Web**
  - 4% of WWW content
  - Also, known as the ‘Visible Web’, it is content that can be found using search engines such as Google or Yahoo. 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.
Surface Web

Deep Web
- Academic databases
- Medical records
- Financial records
- Legal documents
- Some scientific reports
- Some government reports
- Subscription-only information
- Some organization-specific repositories

Dark Web
- TOR
- Political protest
- Drug trafficking and other illegal activities

96% of content on the Web (estimated)
WHAT IS DARK WEB?

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. 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. 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.
HOW TO ACCESS IT?

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, 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.

Do not fool yourself and think that the ISP’s (Internet Service Providers) and Law Enforcement 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 for them.

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 gain access 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.
APPLICATIONS:

The influence of Bitcoin:

The Silk Road became one such popular website on the Dark Web. Known also as the “eBay of drugs”, it is a place to buy and sell things – but mainly illegal drugs.

This was made possible by the use of Bitcoin, a virtual currency that makes use of the encrypted peer-to-peer system.

Bitcoin allows users to conduct business transactions anonymously. This has allowed some users of the currency to engage in illegal activity.

- 2006
  - First Bitcoin traded
- 2011
  - JAN – Silk Road founded by the user ‘Dread Pirate Roberts’
  - FEB – Bitcoin triples in value
  - JUN – US senate investigates link between Bitcoin and Silk Road
  - NOV – Bitcoin loses over 90% of its value
- 2013
  - OCT – FBI locate and arrest the person accused of being the ‘Dread Pirate Roberts’. Silk Road is shut down.
  - NOV – Silk Road 2.0 founded

Bitcoin triples in value*

*Bitcoin is known to be a volatile currency, even though its value has on average constantly increased since its inception, it is prone to large fluctuations in perceived value.

Over $1 billion worth of goods were sold on Silk Road before it was shut down.
Darknet markets:
Commercial darknet markets, which mediate transactions for illegal drugs and other goods, attracted significant media coverage starting with the popularity of Silk Road and Diabolus Market its subsequent seizure by legal authorities. Other markets sell software exploits and weapons. Examination of price differences in Dark web markets versus prices in real life or over the World Wide Web have been attempted as well as studies in the quality of goods received over the Dark web. One such study performed on the quality of illegal drugs found in Evolution, one of the most popular cryptomarkets active from January 2014 to March 2015. An example of analytical findings included that digital information, such as concealment methods and shipping country, seems accurate," but the illicit drugs purity is found to be different from the information indicated on their respective listings." Less is known about consumer motivations for accessing these marketplaces and factors associated with their use.

A darknet market or cryptomarket is a commercial website on the dark web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, other illicit goods as well as the sale of legal products. In December 2014, a study by Gareth Owen from the University of Portsmouth suggested the second most popular sites on Tor were darknet markets.
Things You Can Buy

1. Drugs

Individual or dealer-level quantities of illicit and prescription drugs of every type are available in the digital underground. The Silk Road, the now-shuttered drug superstore, did $200 million of business in 28 months.

2. Counterfeit Currency

Fake money varies widely in quality and cost, but euros, pounds, and yen are all available. Six hundred dollars gets you $2,500 in counterfeit U.S. notes, promised to pass the typical pen and ultraviolet-light tests.

3. Forged Papers

Passports, driver’s licenses, citizenship papers, fake IDs, college diplomas, immigration documents, and even diplomatic ID cards are available on illicit marketplaces such as Onion Identity Services. A U.S. driver’s license costs approximately $200, while passports from the U.S. or U.K. sell for a few thousand bucks.

4. Firearms, Ammunition, and Explosives

Weapons such as handguns and C4 explosives are procurable on the Dark Web. Vendors ship their products in specially shielded packages to avoid x-rays or send weapons components hidden in toys, musical instruments, or electronics.

5. Hitmen

Service providers—including a firm named for the H.P. Lovecraft monster C’thulhu—advertise “permanent solutions to common problems.” For everything from private grudges to political assassinations, these hired guns accept bitcoin as payment and provide photographic proof of the deed.

6. Human Organs

In the darker corners of the Dark Web, a vibrant and gruesome black market for live organs thrives. Kidneys may fetch $200,000, hearts $120,000, livers $150,000, and a pair of eyeballs $1,500.
Things That Make Internet Crime Work

1. Cryptocurrency

Digital cash, such as bitcoin and darkcoin, and the payment system Liberty Reserve provide a convenient system for users to spend money online while keeping their real-world identities hidden.

2. Bulletproof Web-hosting Services

Some Web hosts in places such as Russia or Ukraine welcome all content, make no attempts to learn their customers’ true identities, accept anonymous payments in bitcoin, and routinely ignore subpoena requests from law enforcement.

3. Cloud Computing

By hosting their criminal malware with reputable firms, hackers are much less likely to see their traffic blocked by security systems. A recent study suggested that 16 percent of the world’s malware and cyberattack distribution channels originated in the Amazon Cloud.

4. Crimeware

Less skilled criminals can buy all the tools they need to identify system vulnerabilities, commit identity theft, compromise servers, and steal data. It was a hacker with just such a tool kit who invaded Target’s point-of-sale system in 2013.

5. Hackers for Hire

Organized cybercrime syndicates outsource hackers-for-hire. China's Hidden Lynx group boasts up to 100 professional cyberthieves, some of whom are known to have penetrated systems at Google, Adobe, and Lockheed Martin.

Many hackers sell their services there individually or as a part of groups. Such groups include xDedic, hackforum, Trojanforge, Mazafka, dark0de and the TheRealDeal darknet market. Some have been known to track and extort apparent pedophiles. Cybercrimes and hacking services for financial institutions and banks have also been offered over the Dark web. Attempts to monitor this activity has been made through various government and private organizations, and an examination of the tools used can be found in the Procedia Computer Science journal. Use of Internet-scale DNS Distributed Reflection Denial of Service (DRDoS) attacks have also been made through leveraging the Dark Web. Many hacking groups such as Code:Green also recruit
Hackers depending on their skills. There are many scams *.onion sites also present which end up giving tools for download which are infected with trojan horse or backdoor.

6. Multilingual Crime Call Centers

Employees will play any duplicitous role you would like, such as providing job and educational references, initiating wire transfers, and unblocking hacked accounts. Calls cost around $10.
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. 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. 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 draw of the dark web is a sense of community and freedom that some don't feel on the surface web.

Some other advantages are:

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.
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.

3. Political Activism

The deepweb 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 deepweb has had a major role in recent historical events such as the Arab spring.

4. Knowledge

The deepweb 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 store fronts (pro-suicide, anti-moralism…) are also stored in the deepweb.

5. Amazing individuals

How we act with the resources we have access to concerns our individual responsibilities and judgement. Certain people in what could be called “the deepweb 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 deepweb a better place.
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.

Some other disadvantages includes:

**Hoaxes and unverified content**

There are reports of crowdfunded assassinations and hitmen for hire. however, these are believed to be exclusively scams. The creator of Silk Road was arrested by Homeland Security
investigations (HSI) for his site and allegedly hiring a hitman to kill six people, although the charges were later dropped.

There is an urban legend that one can find live murder on the dark web. The term "Red Room" has been coined based on the Japanese animation and urban legend of the same name. However, the evidence points towards all reported instances being hoaxes.

On June 25, 2015, a creepy indie game Sad Satan was reviewed by Youtubers Obscure Horror Corner which they claimed to have found via the dark web. Various inconsistencies in the channel's reporting cast doubt on the reported version of events.

**Phishing and scams**

Phishing via cloned websites and other scam sites are numerous, with darknet markets often advertised with fraudulent urls.

**Illegal and ethically disputed pornography**

There is regular law enforcement action against sites distributing child pornography – often via compromising the site by distributing malware to the users. Sites use complex systems of guides, forums and community regulation. Other content includes sexualised torture and killing of animals and revenge porn.

**Terrorism**

There are at least some real and fraudulent websites claiming to be used by ISIL, including a fake one seized in Operation Onymous. In the wake of the November 2015 Paris attacks an actual such site was hacked by an Anonymous affiliated hacker group GhostSec and replaced with an advert for Prozac. The Rawti Shax Islamist group was found to be operating on the dark web at one time.
CONCLUSION:

- The deep web will continue to perplex and fascinate everyone who uses the internet.
- It contains an enthralling amount of knowledge that could help us evolve technologically and as a species when connected to other bits of information.
- And of course, it’s darker side will always be lurking too, just as it always does in human nature.
- The deep web speaks to the fathomless, scattered potential of not only the internet, but the human race, too.
- Regardless of if the Dark Web exists or not, the aforementioned activities still occur. The Dark Web just provides an easy way to connect with people of similar interests, and to facilitate further interaction.