WIE GAZETTE

WOMEN • TECHNOLOGY • INSPIRATION • EMPOWERMENT

IEEE Women in Engineering

Wie

VOL-VI

JULY 2021

INDEX

1. Glossary *by Saipriya Rajagopal*
2. Headlines *by Tisha Chawla*
3. Timeline *by Haripriya Bangaru*
4. Women-in-Tech Blog *by Devanshi Jajodia*
5. Learning Guide *by Shreya Thaplyal*
6. Myth Buster *by Muskan Bansal*
7. Gizmo *by Akshata Bhat*
8. Summary *by Ishita Chauhan*
9. FAQs *by Vasundhara Polya*
10. Spotlight *by Navami S*
11. Performers of the Month *by Suhasini Shrivastava*

THEME- DEEP WEB

The deep web refers to parts of the Internet not fully accessible through standard search engines like Google, Yahoo, and Bing. The deep web includes pages that were not indexed, fee-for-service (FFS) sites, private databases, and the dark web.

GLOSSARY

With the internet growing and rooting itself into society faster and faster each day, it goes without saying that it has becom nest; a personalized habitat to access its enormous medley of tricks and twists. This cyber web of information that we build networks upon synchronizes itself to match our requirements, thereby eradicating the need for us to delve deeper than the s vast virtual ocean. However, unbeknownst to most of us living in its superficial paradise, lies a much more elusive and cryp part of it, known as the Deep Web. The Deep web is a collection of those areas of the internet that require a high level of sp terms of software applications and their subsidiaries to be accessed. This particular sphere of the internet has its own vocab definitions to describe its abstruse parts and processes. Let's take a look at some of the most common ones.

1. Botnet

The botnet is a collection of interconnected computers, all infected by a common virus, that allows the owner of it to be abl remotely control the infected devices through its webwork.

2. Carding

Carding is a process referring to the theft of credit card numbers and subsequently selling the obtained information illegally

3. Canary

Canary trapping is a process used to covertly identify sources of information leaks by providing imitations of documents th generally be the target of IP thefts.

4. Honeypot

Honeypots are special virtual traps set by ethical hackers and cybersecurity specialists that involve setting up an imitation c computerized system that resembles targets that would typically attract cybercriminals to attack.

5. Encryption

This is the process of transforming data, called plaintext, into an equivalent yet cryptic form known as ciphertext, which co code that can only be deciphered by the authorized owner to give the original form of data.

6. Firewall

A firewall is a cybersecurity system that supervises and regulates all the networks and their subsequent traffic that gain acc and leave the device.

7. Keyloggers

Certain programs known as keyloggers are disguised as normalized surface web pages and programs that keep track of the undertakings through a recording of their individual keystrokes and patterns. This is then used to access their personal infor which would then be transferred to unethical hackers.

8. Ransomware

Ransomware is a type of computerized malware that locks up the personal information of users on the internet and indicate consequence of exposing the withheld information if a certain ransom is not paid within the stipulated time.

9. Sandbox

Sandboxing is a cybersecurity mechanism that ensures programs on the device being used are compiled and executed in iso environments, blocking its access from the rest of the device. This ensures that in the case of potential malware entering the part of a program, it will not be able to affect any other part of the computer.

10. Spoofing

Spoofing is a process used by cybercriminals to obtain personal information like bank account details and credit numbers, b common communication means like e-mails to appear as if they come from the user's authorized organization, to lure them clicking links embedded with malware.

References:

1. https://whatis.techtarget.com/definition/deep-Web
2. https://www.lifelock.com/learn-identity-theft-resources-what-is-the-dark-web.html
3. https://iaca-darkweb-tools.com/dictionary/
4. https://vpnoverview.com/privacy/anonymous-browsing/dark-web-dictionary/

HEADLINES

Since its inception, the Deep Web has been a vault of all immorality and blasphemy present in the virtual world. With its evolving trends and cutthroat techniques, it has continued to stay alive and chisel out the worst in the public. By evading censorship around the globe, the deep web has steered away from the limelight of authentic web surfing. The platform stages several destructive acts, degrading the morals of the society with its immense power.
There are more than a billion standard web pages that are accessible to the general public. However, these websites only constitute a small segment of the actual internet. The number of these domains is growing with leaps and bounds and includes everything from databases, businesses to freewheeling Deep Web markets.

Let's take a look at some of the evolving trends of the Deep Web.

Rise of Double Extortion Ransomware
In early 2020, there was an increase in the "double-extortion" attacks by some of the more influential ransomware families. These attacks are characterized by a combination of undesirable encryption of sensitive data by fraudulent actors and extrusion of the crucial files to hold for ransom. Following the same trends, many groups switched to a double extortion model throughout the year by encoding the data for ransom and then threatening to release it on social networking sites. Since late 2019, ZeroFox has tracked the cause of Tor-hosted leak sites which were set up by ransomware gangs to dump the data of non-compliant users. Netwalker, Revil, Maze, and DoppelPaymer also began standing up their sites earlier in the year 2020. Besides unauthorized data transfer, some groups used different strategies like victim shaming through advertisements, Distributed Denial of Service attacks, and cold-calling on refusal to pay.

Social Engineering Fodder is Openly Exchanged
In 2019, there's been a remarkable increase in the sale of digital identities belonging to victims infected by malicious software. Each digital profile includes the following details like login credentials for online banking, file hosting, networking, web cookies, browser details, and HTML5 canvas fingerprints.
Social engineering attacks are becoming more targeted each day. The latest wave is resistant to any form of defense other than sophisticated behavioral analytics. Direct extrusion attempts against high-profile individuals and attacks against trusted parties are becoming increasingly common these days. Moreover, some threat actors are purchasing an entire digital identity in one transaction without much authentication.

Exposure of personal data
The deep web exposes organizations to phishing attacks, email compromise, and account takeovers. Criminals tend to target victims more accurately and make them vulnerable. The cost of a single personal record can drop to $1.00, whereas the average price for a single personal record was $8.37. It illustrates the importance of organizations to detect illegal data to reduce damage. Also, legal authorities should prevent it from ever being used effectively as an instrument for cybercrimes.

Bibliography
https://blog.cybersixgill.com/top-4-dark-web-trends-to-watch-for-in-2020
https://www.secureworld.io/industry-news/dark-web-stories
https://www.idagent.com/blog/covid-19-and-the-state-of-the-dark-web-2020/
https://portswigger.net/daily-swig/dark-web

TIMELINE

1960s- Formation of ARPANET or Advanced Research Projects Agency Network, which was a computer network created as an experiment as the predecessor of the Internet and later on the dark web.
1970s-

- First illegal transaction using ARPANET.
- Increased demand for private Internet access away from under the government's umbrella.

1980s- The introduction of the Internet brought along the formulation of "data havens", where data is stored.
1990- Tor, a private Internet browsing network gradually began developing.
1991- Public availability of the Internet and a boom of the Dot-Com bubble.
1992- Origin of Onion Routing, enabling anonymous communication and funded by the US federal government.
1994- Jill Elsworth used the term "Invisible Web" in *The Journal of Electronic Publishing*, referring to websites not registered with search engines.
2000- Release of Freenet, which allowed anonymous browsing and file sharing as free software.
2001- The term "Deep Web" was used for the first time in the 2001 Bergman Study.
2002- The publication of Tor, which significantly played a role in the emergence of the Dark Web after onion routing was patented.
2003- 12P peer-to-peer network was derived from Freenet.
2005- Sitemap Protocol develops and is introduced by Google which is a mechanism permitting users to discover Deep Web resources along with OAI-PMH.
2006- The Tor Project was founded as a nonprofit organization.
2008- Tor2web was designed as a proxy application allowing deep web links to appear followed by the .onion domain.
2009- Invention of Bitcoin. Illegal business on the Deep Web was difficult to complete before the release of cryptocurrency.
2010- During the Arab Spring, Tor facilitated access to critical information and blocked websites by activists and protestors.
2011-

- Evolution of Silk Road rapidly gained popularity for the selling and buying of desired products on the Deep Web, hosting around 12 million transactions.
- Intute, a search engine used to access the Dark Web runs out of funding and becomes a static archive.

2012- LinkedIn and Yahoo! accounts breached using Deep Web.
2013-

- Silk Road shut down by the FBI after it was caught for being a dark web marketplace for drugs.
- Demand for tools to protect against mass surveillance accelerated as Tor assisted in Snowden's whistleblowing.
- Scirus, a search engine used to access the Deep Web, retires.

2015-

- The shutdown of PlayPen, a dark website used for distributing child pornography.
- Ulbricht (founder of Silk Road) was found guilty and sentenced to life.
- Midyear 2015- ISIS uses the dark net to recruit and raise money.

2017-

- Freedom Hosting II, the Dark Web's largest hosting site, is taken down.
- Law enforcement fights cybercrime by dismantling AlphaBay.

2019-

- Billions of breached records made available for free.
- Threat actors use alternate channels to conduct business.

Sources:
https://en.wikipedia.org/wiki/Deep_web
https://www.soscanhelp.com/blog/history-of-the-dark-web
https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/from-tor-to-ulbricht-the-deep-web-timeline
https://www.soscanhelp.com/blog/history-of-the-dark-web
https://www.groupsense.io/resources/dark-web-timeline

TIMELINE

1960s- Formation of ARPANET or Advanced Research Projects Agency Network, which was a computer network created as an experiment as the predecessor of the Internet and later on the dark web.
1970s-

- First illegal transaction using ARPANET.
- Increased demand for private Internet access away from under the government's umbrella.

1980s- The introduction of the Internet brought along the formulation of "data havens", where data is stored.
1990- Tor, a private Internet browsing network gradually began developing.
1991- Public availability of the Internet and a boom of the Dot-Com bubble.
1992- Origin of Onion Routing, enabling anonymous communication and funded by the US federal government.
1994- Jill Elsworth used the term "Invisible Web" in *The Journal of Electronic Publishing*, referring to websites not registered with search engines.
2000- Release of Freenet, which allowed anonymous browsing and file sharing as free software.
2001- The term "Deep Web" was used for the first time in the 2001 Bergman Study.
2002- The publication of Tor, which significantly played a role in the emergence of the Dark Web after onion routing was patented.
2003- 12P peer-to-peer network was derived from Freenet.
2005- Sitemap Protocol develops and is introduced by Google which is a mechanism permitting users to discover Deep Web resources along with OAI-PMH.
2006- The Tor Project was founded as a nonprofit organization.
2008- Tor2web was designed as a proxy application allowing deep web links to appear followed by the .onion domain.
2009- Invention of Bitcoin. Illegal business on the Deep Web was difficult to complete before the release of cryptocurrency.
2010- During the Arab Spring, Tor facilitated access to critical information and blocked websites by activists and protestors.
2011-

- Evolution of Silk Road rapidly gained popularity for the selling and buying of desired products on the Deep Web, hosting around 12 million transactions.
- Intute, a search engine used to access the Dark Web runs out of funding and becomes a static archive.

2012- LinkedIn and Yahoo! accounts breached using Deep Web.
2013-

- Silk Road shut down by the FBI after it was caught for being a dark web marketplace for drugs.
- Demand for tools to protect against mass surveillance accelerated as Tor assisted in Snowden's whistleblowing.
- Scirus, a search engine used to access the Deep Web, retires.

2015-

- The shutdown of PlayPen, a dark website used for distributing child pornography.
- Ulbricht (founder of Silk Road) was found guilty and sentenced to life.
- Midyear 2015- ISIS uses the dark net to recruit and raise money.

2017-

- Freedom Hosting II, the Dark Web's largest hosting site, is taken down.
- Law enforcement fights cybercrime by dismantling AlphaBay.

2019-

- Billions of breached records made available for free.
- Threat actors use alternate channels to conduct business.

Sources:
https://en.wikipedia.org/wiki/Deep_web
https://www.soscanhelp.com/blog/history-of-the-dark-web
https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/from-tor-to-ulbricht-the-deep-web-timeline
https://www.soscanhelp.com/blog/history-of-the-dark-web
https://www.groupsense.io/resources/dark-web-timeline

BLOG

Dark web and human trafficking:

In May 2021, 4 people were arrested in the takedown of a dark web child abuse platform that had over half a million users. This platform known as Boystown was taken down by an international task force which was set up by the German Federal Criminal Police (Bundeskriminalamt) including Europol and law enforcement agencies from the Netherlands, Sweden, Australia, Canada, and the United States. This site's main focus was on the sexual abuse of children and it had garnered about 400 000 registered users when it was taken down.

The surface web which all of us are familiar with and use on a daily basis only takes up 0.03% of the internet. The deep web is the hidden portion of the internet that is accessible only through special search engines due to the presence of added layers of encryption. The dark web is an even smaller fraction of the deep web which is where most fraudulent and illegal activities take place.

With about 2.5 million daily visitors, the dark web has become a new frontier for human trafficking. It is a perfect sanctuary for criminal organizations and terror groups to communicate, advertise and buy or sell anything, including humans. The dark web, just like the name suggests, is misused by criminals who are involved in illegal transactions of drugs, bombs, weapons, body parts, and many more.

Unprecedented technological accessibility and the anonymity that the dark web offers have also led to an upsurge in disturbing materials online including child pornography. Out of all the above-mentioned crimes, human trafficking is the most lucrative crime. According to US research, traffickers spent about $250 million to post over 60 million advertisements, in anywhere between 30,000 and 40,000 Dark-Web pages in a two-year time period. According to the U.N., trafficking nets $150 billion a year.

The perks that the dark web offers ensure complete obscurity of the buyer and seller and it is usually very difficult for concerned authorities to track them down. The trade can be carried out by exchanging bitcoins which, unlike regular financial transactions, is very tricky to monitor. Similarly, IP addresses are concealed in the deep web which is yet again beneficial to traffickers as their true identities remain hidden.

Minimal risk of detection and prosecution of technology-facilitated human trafficking compared with traditional, forms of trafficking make online sex trafficking an attractive illegal activity. One child or girl can make several thousand dollars a day for her traffickers as they can subject her to daily torture and repeated sale unlike other crimes like drug trafficking.

The dark web is not made up of loosely connected people coming together for a similar cause. In fact, it has a well-structured framework behind it which makes carrying out illicit activities seamless for its users. Law enforcement in such cases also becomes a daunting task. Unless we come up with a better solution to track users on the dark web, it continues to remain a threat to human society and race.

LEARNING GUIDE

There is a deep web world that is unknown and less explored. Much like the deep seas. The Internet or rather the World W Web is much bigger than we realize. More than 90% of the World Wide Web- its sites and resources- are inaccessible thr standard browsers like google and bing. They are all a part of The Deep Web. Most of these sites have the extension *.oni* can be accessed through the Tor browser(The Onion Router). To get started on your journey of learning the deep web, yo refer to the following:

1. Tutorials
   a)https://www.youtube.com/watch?v=fUjSVrh9UN4&list=PLCZzKt89aPS-w5A6uGxGlxKcf4ovZHWEA&index=1
   b)https://www.udemy.com/course/deep-web/
   c)https://www.youtube.com/watch?v=4pIi9yTWuRw

2. Playlist
   a)https://www.youtube.com/playlist?list=PLzH6n4zXuckpPcCIJigThQgx5CB5gPiC6
   b)https://www.youtube.com/playlist?list=PL812Qd7G4CzCZ3vUa_acZsSfx4QxR_ovk

3. Certification course
   a)https://www.darkwebacademy.com/courses/dark-web-foundations
   b)https://www.udemy.com/course/the-ultimate-dark-web-anonymity-privacy-security-course/?ranMID=39197&ranEAID=k*VTdGlCbXg&ranSiteID=k.VTdGlCbXg-HX84HhVL39UZXpuXXSKL9A&LSNPUBID=k*VTdGlCbXg&utm_source=aff-campaign&utm_medium=udemyads
   c)https://www.udemy.com/course/the-complete-introduction-to-the-deep-web/?ranMID=39197&ranEAID=k*VTdGlCbXg&ranSiteID=k.VTdGlCbXg-7qnDRqyB_exVc0_S_COqEA&LSNPUBID=k*VTdGlCbXg&utm_source=aff-campaign&utm_medium=udemyads
   d)https://www.udemy.com/course/ultimate-deep-web-guide/?ranMID=39197&ranEAID=k*VTdGlCbXg&ranSiteID=k.VTdGlCbXg-ebUS6x4rLFm731QlzJU0nA&LSNPUBID=k*VTdGlCbXg&utm_source=aff-campaign&utm_medium=udemyads
   e)https://www.udemy.com/course/the-deep-web/?ranMID=39197&ranEAID=k*VTdGlCbXg&ranSiteID=k.VTdGlCbX ErUdHRXoXRyl0quuUVfTHQ&LSNPUBID=k*VTdGlCbXg&utm_source=aff-campaign&utm_medium=udemyads

4. Recommended books
   a)Weaving the Dark WebLegitimacy on Freenet, Tor, and I2P By Robert W. Gehl(https://mitpress.mit.edu/books/w dark-web)
   b)Tor And The Deep Web: The Complete Guide To Stay Anonymous In The Dark Net: Two Manuscripts In one (https://www.amazon.in/Tor-Deep-Web-Complete-Manuscripts-ebook/dp/B07B66SMN2)
   c)Tor and the Dark Art of Anonymity: How to Be Invisible from NSA Spying(https://www.amazon.com/dp/1512049581?tag=uuid10-20)

5. Software Required
   Tor download link:
   https://www.torproject.org/download/

MYTH BUSTER

1. The biggest myth that surrounds the **Deep Web is that it is the same as the Dark Web**.
Although some people might use these two terms interchangeably, they do not mean the same thing. The Dark Web is structured with the objective of protecting the privacy of each individual using it. This objective is abused by criminals to perform illegal activities and trade. Whereas, the Deep Web contains information that cannot be accessed easily by search engines or is not linked publicly which makes this content harder to find or uncover. For example, a page that appears when you log in to any website is part of the Deep Web, other pages such as pop-ups are also counted as part of the Deep Web.
It is estimated by experts that the deep web accounts for more than 90 percent of the internet while the dark web is only 0.1 percent.

2. Many times, the media and news portray **the Deep Web as illegal and run by criminals**. This is only fiction. In reality, the Deep Web is entirely lawful and legitimate, most often it is run by renowned and trustworthy individuals and companies. For instance, when you log in using your credentials to check your bank account or medical reports, the web page that appears isn't searchable on Google. Thus, making it a part of the Deep Web. Generally, non-indexed web pages are confused as part of the Dark Web, which promotes privacy.

3. It is believed that **special tools are needed to access the Deep Web**.
Technically, the Deep Web contains standard pages that only require a basic web browser that a person uses daily such as Microsoft Edge, Google Chrome. But in order to access the Dark Web special browsers are required.

4. Movies and media have forced a lot of people into believing that the **Deep Web is only for experts.**
But the truth is that most of the common public utilizes the dark web on a daily basis to access their emails because one needs to first login their details such as email address and password and then securely use a platform like Gmail or Outlook.

5. The last misconception about the **deep web is that it is completely anonymous**.
Confusing the concept of the dark web with the deep web, people believe that their identity is a complete secret on the deep web. But using the Deep Web does not hide your online footprint or guarantee complete anonymity.

GIZMO

All websites that are unidentified by search engines are referred to as "deep web."Passwords or other security barriers may be used to secure deep websites, or they may simply direct search engines not to "crawl" them. For a variety of reasons, some pages are more hidden owing to the absence of obvious links.

1. DeepPeep:

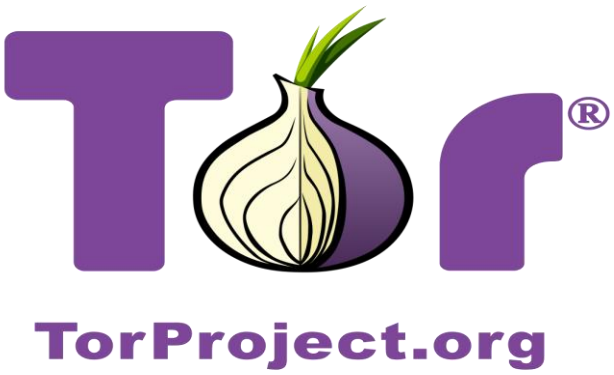
   DeepPeep was a search engine to crawl and index every database on the Internet. Unlike typical search engines, which trawl existing websites and hyperlinks, DeepPeep sought to provide access to the so-called Deep web, which consists of World Wide Web material that can only be accessed by entered queries into databases. Juliana Freire, an associate professor at the university's School of Computing WebDB department, led the project at the University of Utah. According to Freire, the objective was to make 90% of all WWW information accessible. The research was funded by the University of Utah and a $243,000 grant from the National Science Foundation, and it included a beta search engine. It sparked international interest.

2. ImmuniWeb:

   ImmuniWeb is a global application security company headquartered in Geneva, Switzerland. It uses its proprietary ImmuniWeb AI Platform to build Machine Learning and AI technologies for SaaS-based application security solutions. For well-informed, DevSecOps-enabled application penetration testing, the ImmuniWeb AI Platform reveals your external attack surface and Dark Web exposure.

3. Tor Browser:

   Tor, which stands for 'The Onion Router,' is an open-source privacy network that allows users to surf the internet anonymously. Before being made available to the general public, Tor was created and only used by the US Navy to filter government communications.



4. Sitemaps:

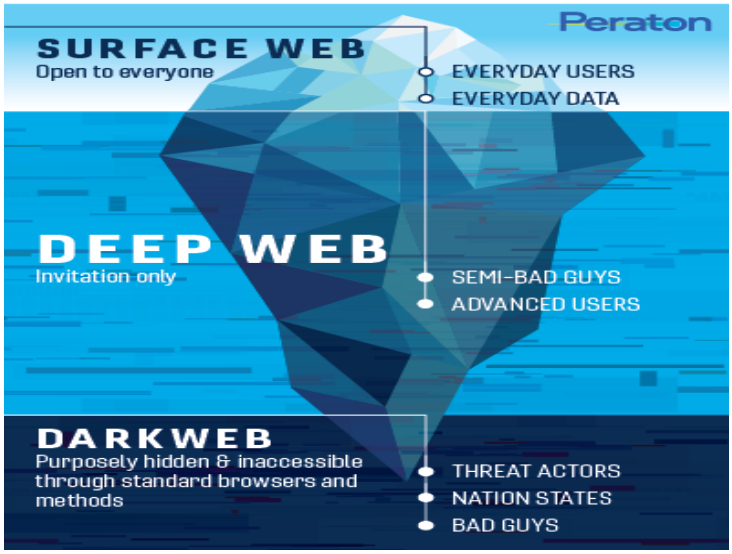
   A webmaster can use the Sitemaps protocol to notify search engines about crawlable URLs on a website. It's an XML file that lists a website's URLs. It allows webmasters to enter details about each URL, such as when it was last updated, how frequently it changes, and how significant it is about other URLs on the site This makes it easier for search engines to scan the site and identify URLs that are separate from the rest of the information.

SUMMARY

The Hidden Part of the Internet-Deep Web:

The Deep Web is a kind of a parallel universe or an alternative Internet which consists of data that isn't indexed by Google or other such search engines. For example, a private Instagram account's content cannot be displayed on searching, and hence it's a part of the deep web.

All search engines use robots to crawl the web and add new content they find to the search engine's index. No one knows for certain how big the deep web is, but many experts estimate that content crawled and indexed by search engines is less than 1% of all content that can be accessed over the internet. Search content on the web is called surface web.

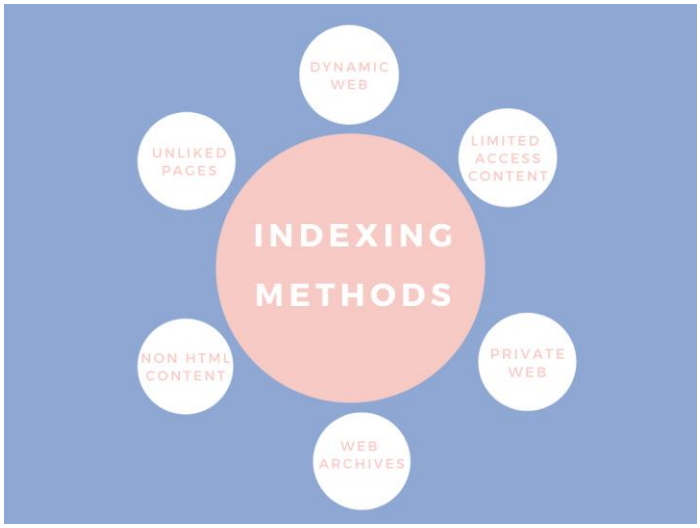


Source: https://www.peraton.com/five-things-to-know-about-the-dark-web/

Indexing Methods

The following are some popular ways in which a webpage can be prevented from being indexed.

- **Dynamic Web**: these are pages that can only be accessed while sending forward a form.
- **Limited Access Content**: this includes sites that protect content through technical means such as Captcha.
- **Private Web**: these are pages that need registration/ login to access data.
- **Unlinked Pages:** this covers pages that aren't backlinked and hence prevents web crawling.



SUMMARY

Dark Web:

The Deep Web is around 300–400 times the size of the internet known to us. A very small and dangerous section of this is the Dark Web. The Dark Web is part of the Deep Web wherein you can maintain absolute anonymity. It is the part that is infamous for being home to weapons, drugs, and even assassins.
Although scary, the Dark Web is doing us all a huge favor. Let's find out how:

1. Trolls and Stalkers
In today's world creeping up on someone is not that hard. It doesn't require a person to physically follow someone and hid behind bushes. All they need is a stable network connection and they can ruin someone's life at the comfort of their home. For example, let's look at Cree.py. It's a geolocation OSINT tool that gathers geolocation-related information from online sources and allows for its presentation on a map, search filtering based on the exact location. It can help keep tabs on active Twitter and Facebook users.
Stalkers in today's world can track your phone by following GPS signals and even turn on the camera and microphone on it.

2. Rampant Commercialisation
Today we might be heading towards a two-tiered internet. It is the end of net neutrality. The internet has become bliss for those who can pay and rubbish for those who can't. Instead of an information superhighway, we are going to be looking at an expensive toll road. We're looking at a pay-TV model. Even if you think something is free, it invariably isn't.

3. Freedom of Speech
We've all heard of the flying rumours that all our actions are being monitored. Sometimes it's the North Korean government and sometimes it's Facebook. What this has done is created a fear in the minds of people which results in them not being able to express themselves freely.

How can it be accessed?

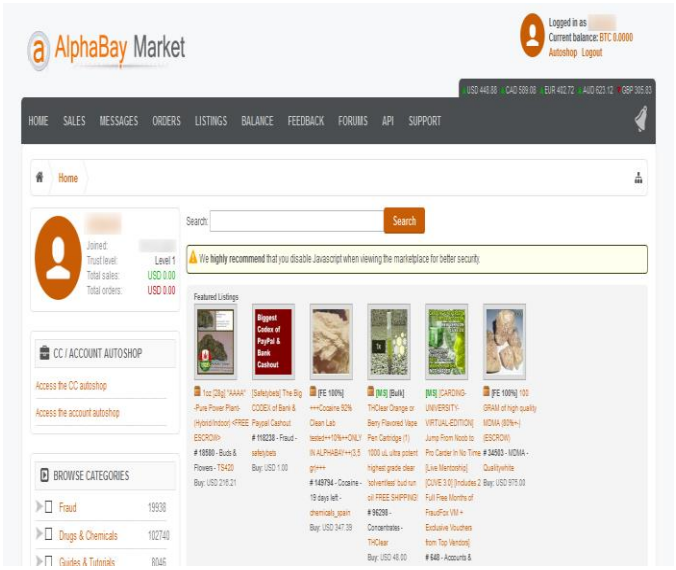
Getting on the deep web is easier than it seems. All you need to do is download a deep web browser such as Tor (The Onion Router). After that, you just treat it as an ordinary browser and search away. However, since it doesn't follow any indexing like Google, it might be a little hard to find what you want.
When you use the Tor network, your traffic is layered in encryption and routed through random relays, where it is wrapped in another layer of encryption. This is done three times through a decentralized network of nodes called circuits: the nodes are run by volunteers who care about privacy, which makes it difficult to track you or the website to see your true location.

In addition to bounce encrypted traffic through random nodes, Tor Browser also clears your browsing history and clears cookies after each session. But it has other clever tricks to deal with trackers. If someone visits two different sites that use the same tracking system, they will usually be tracked at the same time. Tor Browser detects such surveillance and turns on each surveillance through a different circuit, making the connection look like two different people, so if a website logs in to one of the sites, the website cannot link activity or identity.
However, Tor has its flaws too...
Although difficult, it is possible to track down someone 's traffic by pinging through Tor nodes. It can be done through the "first contact problem" which is when the attacker discovers that someone has moved from a non-private tool to a private tool.

Some popular dark web criminal cases:

1.Silk Road
Created by Ross Ulbricht, Silk Road became huge with an idealist wanting to sell homegrown mushrooms for bitcoins. In the process, he found himself in deals worth over 1.2 billion dollars involving firearms, hacker tools, and drugs. However, the site was closed down when Ross was found promoting Silk Road on a normal website while using his actual email address.
2. AlphaBay
Just after the Silk Road was closed, AlphaBay became the new marketplace. However, this too saw a downfall when its creator Alexandre Cazes used a real email address for communications and re-used the same across on and off AlphaBay.

SUMMARY



Source:
https://medium.com/@marcell74/the-silk-road-a-real-thriller-and-the-truth-about-the-anonymity-of-bitcoin-198b519ca397
https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/

How to be careful

Here's how you can keep yourself safe while surfing on the dark web.

- Detaching your real persona from your online persona
- Make use of active monitoring to avoid theft of identity
- Use a VPN
- Use only cryptocurrencies for transactions
- Install TAILS- Amnesic Incognito Live System to avoid leaving traces

References:

1. https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html
2. https://medium.com/@marcell74/the-silk-road-a-real-thriller-and-the-truth-about-the-anonymity-of-bitcoin-198b519ca397
3. https://privacysavvy.com/security/safe-browsing/dark-web-safety/
4. https://en.wikipedia.org/wiki/Deep_web
5. https://www.hackread.com/8-best-dark-web-search-engines-for-2020/
6. https://thehackernews.com/2016/02/deep-web-search-engine.html
7. https://www.kaspersky.com/resource-center/threats/deep-web
8. https://whatis.techtarget.com/definition/deep-Web
9. https://www.wired.co.uk/article/what-is-the-dark-web-how-to-access
10. https://readwrite.com/2008/12/22/contextual_web/?__cf_chl_jschl_tk__=pmd_dc77c07289662a04a43392ea99b3eb4315fa6ea7-1627398652-0-gqNtZGzNArijcnBszQo6

FAQs

1. What is the difference between the dark web and the deep web?
The deep web consists of websites that are not indexed and thus inaccessible to crawler-type search engines like Bing and Google. The dark web is a small portion of the deep web that can be accessed only through specific softwares like Tor as the IP addresses are hidden which allows anonymity of the user and their location.

2. Are the contents of the deep web completely inaccessible?
No. Simply put, the deep web consists of information that is not accessible to the general public due to security or other reasons. For instance, the bank details of individuals are stored on the deep web and can be retrieved only by specific authorities, software or configurations.

3.What does the deep web typically consist of?
The deep web mainly consists of massive databases and internal networks of various organizations like academic institutions, hospitals, banks, and so on. Netbanking details, research papers, medical records, private forums, etc. are stored on the deep web. To adumbrate, the deep web comprises internal networks and websites which are not indexed by commonly used search engines.

4. How safe is it to use the deep web?
The deep web is comparatively safer than the dark web. But to be on the safer side, it is always recommended to practice safe internet habits. Since the deep web contains a humongous amount of personal information which cybercriminals might find useful, it is a good practice to not access confidential information on an unprotected public network. Using a virtual private network (VPN) will encrypt your data thus safeguarding online privacy.

5. Is the dark web illegal?
The dark web in itself is not illegal. The dark web consists of websites whose IP addresses are purposefully hidden making it impossible for normal users to trace. It ends up serving as a host for many illegal activities to take place due to the lack of traceability. A cybercriminal may choose to hack someone's confidential data, sell it on the dark web without being traced.

6. Why is the deep web not as popular as the surface web?
Lack of adequate knowledge, safety, and requirements are the key reasons for the limited popularity. The myth that deep web and dark web are synonymous, safety concerns over the data accessed through the deep web being hacked might prevent individuals from exploring the deep web. Secondly, the surface web provides users with a plethora of information which is sufficient for many users. Therefore, everyone might not find it necessary to use the deep web.

Bibliography:

1. https://www.alphonsolabs.com/does-the-deep-web-exist/
2. https://www.lastpass.com/solutions/dark-web-monitoring/faqs
3. https://www.techlazy.com/the-deep-web-dark-web-a-beginners-guide/
4. https://www.hexacta.com/6-questions-about-deep-web/
5. https://deepweblinks.net/how-to-access-the-deep-web/

SPOTLIGHT

Domain: Editorial

In a digital era, where almost all aspects of commerce, industry, and life depend upon the usage of gadgets and the knowledge of various advancements in the field of technology, the power of print media in spreading awareness about the newest updates on the latest tools, filtering and reviewing products and software is, without a doubt, undeniable. IEEE-WIE is a technical chapter divided into 4 major departments, namely technical, design, management, and editorial department, which has some of the best designers, developers, and tech enthusiasts who collaborate to push technology forward and foster a community of women tech enthusiasts. Editing involves the process of publishing technical content, staying consistent, and checking if the submissions are concise, technically accurate, and unbiased. In the IEEE-WIE chapter of VIT, the Editorial Domain plays that role. We publish blogs as well as a monthly newsletter- WIE Gazette. In this edition of the WIE Gazette, I was given the opportunity to interact with the marvellous **Editorial Head** in the IEEE-WIE chapter of VIT, **Vrushali Deshmukh**. She is undoubtedly one of the most diligent and committed individuals in the chapter who works tirelessly with the domain members to produce original content. In this interview, she gives us an insight into the various activities that shape her position in the Editorial Domain.

Q1. Can you give us an overview of the tasks that you are responsible for as the Editorial Head? How do you find a balance and ensure their completion?

Vrushali: As the editorial head of IEEE-WIE, the first thing that I'm responsible for is to publish blogs, which involves ensuring that the articles have been written at least a week before the deadline so that proper proofreading for any errors, putting them up on Medium, adding relevant hashtags, delegating the role of adding captions and description to the submissions can all be executed on time. Gazette is a monthly newsletter with 11 pieces. I filter the submissions, review the content for relevancy and technical accuracy and then finally put them up on our website. Finding a balance can be challenging sometimes, but by setting realistic deadlines, I provide the writers the time and space to complete their assigned work. The work is distributed among the entirety of the editorial department which ensures that nobody is overworked. Proper follow-ups help in staying updated with the progress.

Q2. What is the fact-checking process like? How do you provide constructive feedback to writers?

Vrushali: The first step to the fact-checking process is to run the submissions through plagiarism checkers and Grammarly checkers to ensure no duplicity. After reading the submissions myself, I send them over to a few others to form a collective opinion on the relevancy of the content present. Constructive feedback is crucial to any workplace. I add comments to the documents, highlight areas where I feel an elaboration is required, and also point out errors. I appreciate and criticize the work at the same time which helps in bringing out the best in everyone. Being polite is key as it helps in not exploiting the writer's creative freedom.

Q3. Editing involves long stretches of proofreading, source checking, indexing, and much more. How do you keep the mundane parts of editing interesting?

Vrushali: I completely agree with the statement that the process is a long stretch of repeated processes that are mundane. To keep it interesting, I take only 2-3 blog pieces at a time so that the work isn't tiresome and also because I can always have a fresh perspective on each piece that helps me provide constructive feedback to its authors. I proofread every piece and also send them to a few others as well which helps me filter better. For source-checking, I read through the articles mentioned under the bibliographical references that the authors provide, so that I can form an idea about the originality of the piece. I provide the author's the freedom to index the piece themselves so that their vision of how the article should look isn't taken away.

Q4. What are some of the challenges of leading the Editorial Department? How do you work around them?
Vrushali: The department faces a lot of obstacles. Perhaps the most challenging of them all would be to ensure that none of the writer's creative freedom is ever snatched away from them. To avoid intruding into their thinking space, I try not to nitpick bits but rather pinpoint wherever I find changes are necessary. Since IEEE-WIE is a technical chapter, writing technical articles is a niche-based activity, which can be a challenge for some due to a lack of familiarity with the style. This sometimes results in the writers not being able to explore beyond the technical world of writing. There can also be instances where the writers need to indulge in a lot of background research which can end up being monotonous and tedious. There can be times in which writers reach a writer's block that hampers both the writing and editing processes that lead to a couple of people working and providing many changes which then need to be filtered. Another challenge would be to get acquainted with everyone's style of writing. Understanding the way they create content and then helping them bring out the best version of their submission is a time-taking and taxing task.

Working around these challenges is crucial in bringing out a well-written piece. Being honest and polite goes hand in hand in ensuring that I get the desired changes made. Being straightforward helps in avoiding confusion. Whenever I encounter a writer's block happening with someone, I provide them enough time to come out of it and also extend my help so that the work is completed on time.

Q5. What advice would you give to tech enthusiasts looking to publish their articles to come up with an impeccable piece of content?
Vrushali: My biggest advice would be to do extensive research before writing a technical piece. After reading, watching, and learning from as many relevant sources as possible, I try to include information about playlists, videos, courses, books, and certifications that the readers can further look into. I ensure that the simplicity of the language isn't compromised as technical articles are more about the content and not the style of writing. Complex sentences with heavy-sounding words would just discourage readers from reading more. So the true test of a technical writer is to present the most complex concepts using the simplest words.

STAR PERFORMERS

1. **Design:**
   Ananya Kondalraj has stunned everybody with her conscientious work and enthusiastic nature.She is granted the member of the month for her imaginative and amazing commitment to the chapter. She is an esteemed individual from the design domain who works hard diligently to plan the astonishing posters for various events.Ananya is unconstrained with regards to volunteering for any event. She makes sure that her designs are alluring. We are absolutely glad to have such an exemplary member like Ananya in IEEE-WIE. Keep ascending the stepping stones to success in the field of design, Ananya!

2. **Editorial:**
   Tisha has been awarded the member of the month for her excellent work in the editorial domain. She is constantly anxious to chip in for any task allotted and has an imaginative way to deal with it. She is a stunning writer and keeps herself refreshed with all the most recent innovation patterns.Tisha has done an extraordinary job in each of the tasks she was assigned- be it writing captions or blog pieces.She also organized an informal event with other core members to promote team bonding. Congrats Tisha!!

3. **Management:**
   The genuine measure of the worth of any supervisor is execution. Shihij has performed extraordinarily well and has been recognized as the member of the month from the management domain. She is reliable with her work and obligations and she ensures that every one of the events is done successfully. Her genuine commitment to the work never stops inspiring others. From organizing occasions to flawlessly driving a group, she is always on top. Her systematization and association abilities are unparalleled and she has consistently ended up being a much-esteemed individual from the club. A major overwhelming applause to you Shihij !!!!

4. **Technical:**
   Priyanka is nominated for the member of the month from the technical domain for her ingenuity and commitment. She has effectively taken interest in all the night meetings and events led by the chapter. She doesn't avoid giving important contributions during club gatherings and is consistently anxious to learn new things. Keep Shining Priyanka!!!

EDITORS

Vrushali Deshmukh- Editor-in-Chief

Saipriya Rajagopal

Suhasini Srivastava

Devanshi Jajodia

Ishita Chauhan

Tisha Chawla

Akshata Bhat

Muskan Bansal

Haripriya Bangaru

Vasundhara Polya

Navami S

Shreya Thaplyal