



Department of Electrical & Computer Engineering

CSE 499B: Senior Design Project

FINAL REPORT

Dark Web – E-commerce sites

Section: 6

Submitted By:

Md. Abdur Rakib Rahat - (ID: 162 0521 042)

Sumaya Yeacin Rimu - (ID: 153 0664 042)

Md. Raihan Hossain - (ID: 161 0456 642)

Anwar Shadaab - (ID: 161 1383 042)

Submission Date: **24th July 2020**

Submitted To:

Mohammad Ashrafuzzaman Khan
(Assistant Professor)

Abstract

Where Dark Web is a much bigger place than our surface web in terms of the number of websites, we cannot say the same thing about the e-commerce world of Dark Web. Most of the e-commerce in Dark Web is linked with various illegal activities. It can be consider as a huge repository of selling drugs, weapons, pornography, personal documents, stolen & brand new electronic parts, even body parts of human. Using transaction via anonymous cryptocurrency, Dark Web assured buyers that they can trade in here without exposing their personal information. Privacy is a key component which makes the e-commerce of Dark Web so popular and it is increasing rapidly. Our purpose of this research is only to observe the structure of e-commerce websites of Dark Web & the main causes which bring the interests of buyers to visit Dark Web e-commerce more & more. And in order do accomplish that, this research paper represents our attempt to crawl, scrape the dark websites.

Table of Contents:

1	Introduction	4
1.1	Why it is dark and not on the same platform	4
1.2	The Problems	5
1.3	Introduction to Dark web E-commerce	6
1.4	Why it is interesting.....	8
1.5	Benefits of doing E-commerce on dark web.....	8
2	Dark Web	9
2.1	History.....	9
2.2	Dark web & the Government.....	14
2.3	Who uses Dark web & why	14
2.4	Is it illegal to access Dark web? How safe if is?	16
3	Dark Web E-Commerce.....	17
3.1	Kind of business are done on Dark web	17
3.2	Demography	22
3.3	Stories/Anecdotes from Dark web Ecommerce.....	26
3.4	Market comparison chart	27
3.5	How Dark web markets are exploiting the Corona virus Pandemic	30
3.6	Dark & Surface Web Search Engine Index	34
4	Experiments	44
5	Acknowledgements.....	47
6	References	47

1 Introduction

The dark web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed. The dark web is a part of the internet that isn't indexed by search engines. You've no doubt heard talk of the "dark web" as a hotbed of criminal activity. The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser—Tor—to access, as explained below. No one really knows the size of the dark web, but most estimates put it at around 5% of the total internet. Again, not all the dark web is used for illicit purposes despite its ominous-sounding name. The anonymity of the dark web makes it an attractive technology for illegal purposes. However, it also hosts many legitimate companies like New York Times and Facebook who offer Tor-based services, as well as generally benign content. The dark web is not synonymous with cybercrime. To clarify, the deep web is broadly defined as anything that is not indexed by traditional search engines. Unsurprisingly, the deep web is also home to criminality – but so too is the clear web. The dark web does not monopolize cybercrime.

The portion of the Internet that is hidden from conventional search engines, as by encryption; the aggregate of unindexed websites is the deep web. And the dark web is the portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser: part of the deep web." The key takeaway here is that the dark web is part of the deep web. What the dark web and the deep web have in common is that they are both hidden from commercial search engines. You cannot access either from Google or Bing. The deep web is a general, catch-all term that includes the dark web, but also includes "mundane content like registration-required web forums and dynamically-created pages like your Gmail account," according to Andy Greenberg at Wired. That is to say, most of the deep web is irrelevant to the news stories about Silk Road.

When people discuss the seedy underbelly of the Internet where you can buy drugs, weapons, child pornography, murders-for-hire—basically any illicit item or service you could dream up—that's the dark web. Greenberg notes that while the deep web is vast and accounts for 90-something percent of the Internet, the dark web likely only accounts for about .01 percent. The dark web, sometimes referred to as Dark Net, is accessed by Tor (The Onion Router) or I2P (Invisible Internet Project), which use masked IP addresses to maintain anonymity for users and site owners. This way, people who use the dark web for illegal purposes can't be traced.

1.1 Why it is dark & not on the same platform

The Structure of the Internet

The internet is broken into three parts, the open, deep, and dark web. Most of us use the open web and deep web daily when we browse our favorite blogs and log into social media. However, the dark web's content is not accessible through "traditional browsers or standard browsing technology" and is designed to be hidden from search engines, preventing them from appearing on the clear web.

Browsing and Privacy

Users are tracked across the clear and deep web via IP (Internet Protocol) address. With this information, website owners can 'see' users' physical locations when accessing their site. IP also allows tracking services to record your website visits – selling this information to marketers who develop ads that "follow" you online. Dark web browsing technology negates these issues by anonymizing traffic. The encrypted

routing technology at the core of the Tor Network, an example of dark web browsing technology, circumvents IP tracking and thus adds a layer of privacy for users online.

As mentioned above, to access and browse the dark web, browsing technology, like the Tor network, is utilized. VPNs, Tor browsers, and even operating systems are leveraged to protect the user from being tracked and identified. Hundreds of communities exist on the dark web, from healthcare to politics, the dark web ecosystem hosts a diverse number of entirely legitimate and legal websites, organizations, e-commerce platforms, and social forum.

Privacy Enables Criminality but Not on Purpose

While the anonymity enjoyed by dark web users serves as a foundation for the thriving dark web fraud economy, the dark web also acts as a shield for persecuted groups, persons under oppressive regimes, and whistleblowers.

The Takeaway: The dark web, practically, is a privacy tool created to protect users' identities while they traverse the internet for various reasons. Cybercriminals are leveraging the dark web to build hidden e-commerce platforms that specialize in the trade of your stolen data, counterfeit goods, and multiple services. These e-commerce platforms are powered by the demand for and availability of sensitive data.

1.2 The Problems

E-commerce sites implement their business strategies using dark web e-commerce sites to using the dark web. In dark web e-commerce sites, the buyer starts with selecting the right product, and it goes all the way past the purchase to dealing with the seller store after the product arrives. Below we've collected some common problems that e-commerce websites suffer from that get in the way of customer satisfaction.

1. **Poor Image:** Most of the time customers that buy the product online have never seen the product. They want to examine things from every angle on their screen. If the image quality doesn't that much good then it is very difficult to buy that product.

2. **Unfriendly Returns:** Online shopping is risky for customers. People don't want to be stuck with items that don't fit or are damaged on arrival.

3. **Slow Speed:** For the costumes, rarely, they don't want to spend too much time buying a product on a page, so slow internet is a big problem for shopping.

4. **Suspicious Reviews:** Manufacturers know that good reviews will increase their chances of a sale. Customers know that reviews will reveal problems with the item they want to buy. But when a product has 100% negative reviews, customers will not take that product.

5. **Poor Content and Product Descriptions:** Many e-commerce stores Product descriptions came into sharp focus since many stores were using thin or generic text. Customers read the content and description before buying it online.

1.3 Introduction to Dark Web E-Commerce

The dark web has flourished thanks to bitcoin, the crypto-currency that enables two parties to conduct a trusted transaction without knowing each other's identity. "Bitcoin has been a major factor in the growth of the dark web, and the dark web has been a big factor in the growth of bitcoin," says Tiquet. Nearly all dark web commerce sites conduct transactions in bitcoin or some variant, but that doesn't mean it's safe to do business there. The inherent anonymity of the place attracts scammers and thieves, but what do you expect when buying guns or drugs is your objective?

Dark web commerce sites have the same features as any e-retail operation, including ratings/reviews, shopping carts and forums, but there are important differences. One is quality control. When both buyers and sellers are anonymous, the credibility of any ratings system is dubious. Ratings are easily manipulated, and even sellers with long track records have been known to suddenly disappear with their customers' crypto-coins, only to set up shop later under a different alias. Most e-commerce providers offer some kind of escrow service that keeps customer funds on hold until the product has been delivered. However, in the event of a dispute don't expect service with a smile. It's pretty much up to the buyer and the seller to duke it out. Every communication is encrypted, so even the simplest transaction requires a PGP key. Even completing a transaction is no guarantee that the goods will arrive. Many need to cross international borders, and customs officials are cracking down on suspicious packages. The dark web news site Deep.Dot.Web teems with stories of buyers who have been arrested or jailed for attempted purchases.

With all that stolen data floating around, hackers have transitioned from using it for themselves, and have begun to sell it to scammers online. Since it is illegal to try and sell unauthorized data it is sold on the Dark Web. Besides special authorization and software to access, which allows users to interact anonymously via Tor browser, the overall experience is very similar to your traditional online shopping experience. As Dark Web is becoming more sophisticated it is starting to adopt some of the principles of the traditional ecommerce retailers. They are offering "autosshop" experience coupled with anonymity. Some sellers even have refund policies! In order to keep transactions anonymous the marketplace operates in Bitcoin, an unmarked and untraceable digital currency, and they often sell their goods at prices cheaper than you'd expect and with the ease of immediate download or shipment. Platforms like these are so much more than just rudimentary command line setups or chat rooms. They offer many of the same features as online stores like Amazon or EBay with vendor ratings, buyer feedback, detailed search options and facilitated transaction and delivery services. Collections of data are presented with detailed descriptions (similar to an ecommerce product pages), and some even provide tutorials on how to best utilize that data to scam victims. Here is an example of the user-friendly design of one store found on the Dark Web, and how openly they shop the information of a yahoo user.

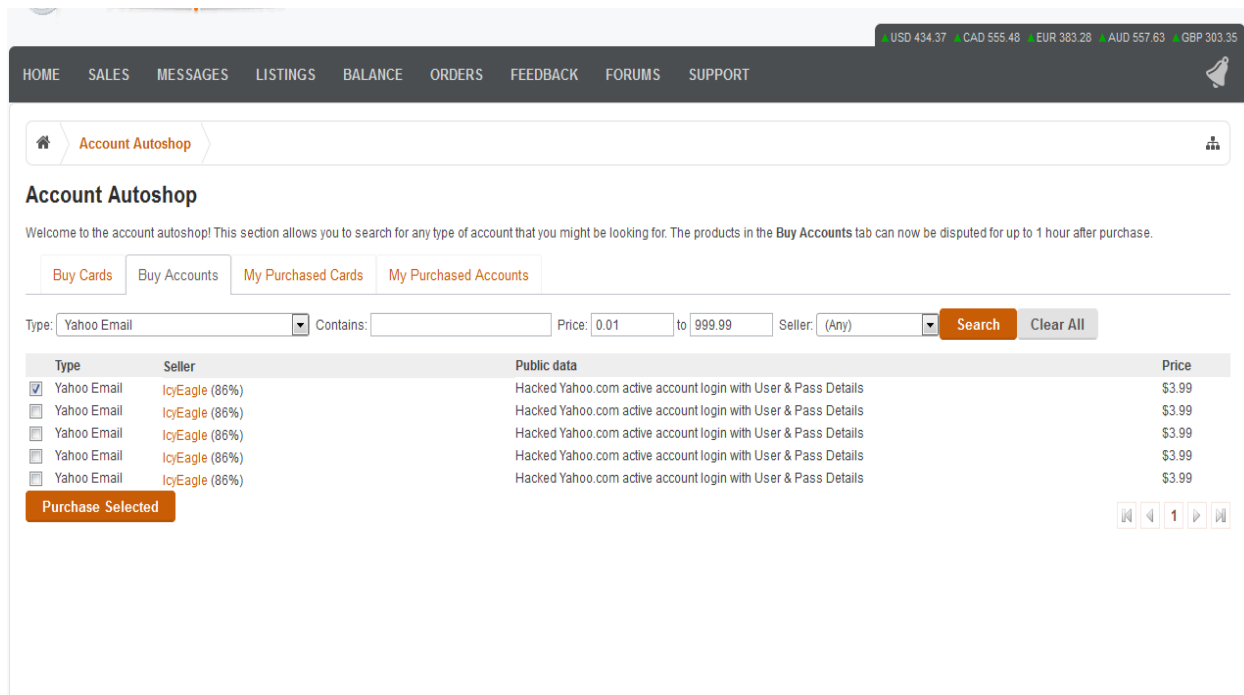


Fig 1: Screenshot of Autoshop (An e-commerce website of Dark Web)

You can see just how easy it is for the Dark Web users to search for products by any number of qualities including category, product type, price, sale type & location and shipping options. The stores are designed to make shopping and buying as easy as possible for scammers and fraudsters.

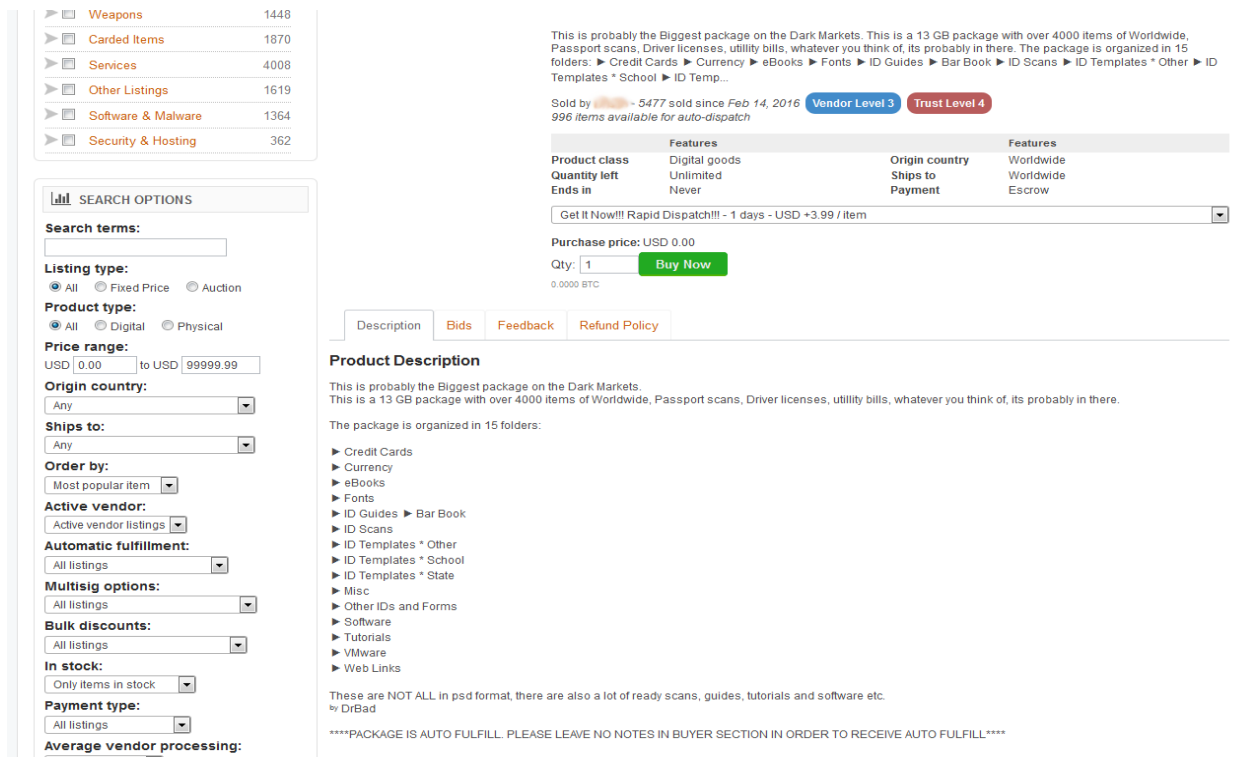


Fig 2: Another e-commerce website of dark web

1.4 Why it is interesting

Today, the Internet is the most used human-built technology and even it is growing more with its full potentialities day by day. Though the Internet of this generation is not only limited to the common purpose to use, it also becomes a part of the crime world too. Many people today are aware of this fact that the Internet is divided into different layers in which each layer of the Internet has its specific purpose of existence. The most common and first part is the Surface Web, therefore the Deep Web comes and at last, the most hidden part of the Internet aka the subset of the Deep Web comes which is named the Dark Web. The Dark Web is made up of websites which requires their browsers for access like TOR, Freenet, and I2P. The Dark Web is the place that hosts the illegal markets and media which the press love to write about. However its main purpose is to provide anonymity to web users.

1.5 Benefits of doing E-commerce on Dark Web

There are some points which can be seen as benefits in order to doing e-commerce on Dark Web:

1. Overcome Geographical Limitations

If you have a physical store, you are limited by the geographical area that you can service. With an e-commerce website, the whole world is your playground.

2. Gain New Customers with Search Engine Visibility

In the physical store seller can have only that area customers and known people and limited customers. But with an online store on dark sites there is no limitation of customers. Anyone can have to look at their products from anywhere in the world.

3. Lower Costs

One of the most tangible positives of e-commerce is the lowered cost. A part of these lowered costs could be passed on to customers in the form of discounted prices. Here are some of the ways that costs can be reduced with e-commerce:

- Advertising and marketing: organic search engine traffic pay-per-click, and social media traffic are some of the advertising channels that can be cost-effective.
- Personnel: The automation of checkout, billing, payments, inventory management, and other operational processes lowers the number of employees required to run an e-commerce setup.
- Real estate: This one is a no-brainer. An e-commerce merchant does not need a prominent physical location.

4. Locate the Product Quicker

It is no longer about pushing a shopping cart to the correct aisle or scouting for the desired product. On an e-commerce website, customers can click through intuitive navigation or use a search box to narrow down their product search immediately. Some websites remember customer preferences and shopping lists to facilitate repeat purchases.

5. Eliminate Travel Time and Cost

It is not unusual for customers to travel long distances to reach their preferred physical store. E-commerce allows them to visit the same store virtually, with just a few mouse clicks.

6. Provide Comparison Shopping

E-commerce facilitates comparison shopping. Several online services allow customers to browse multiple e-commerce merchants and find the best prices.

7. Remain Open All the Time

Store timings are now 24/7/365. From the merchant's point of view, this increases the number of orders they receive. From the customer's point of view, an "always open" store is more convenient.

8. Create Markets for Niche Products

Buyers and sellers of niche products can find it difficult to locate each other in the physical world. Online, it is only a matter of the customer searching for the product in a search engine. One example could be the purchase of obsolete parts. Instead of trashing older equipment for lack of spares, today we can locate parts online with great ease.

2 Dark Web

The Deep Web and its Dark Web subset have been in the public eye more than usual in the past few years. Once the things that happen on the hidden part began having an impact on the "real" world, regular Joes and Janes started to take an interest. That doesn't mean the hidden part of the internet is a recent development. It's just about as old as the internet itself!

2.1 History

The Early Days

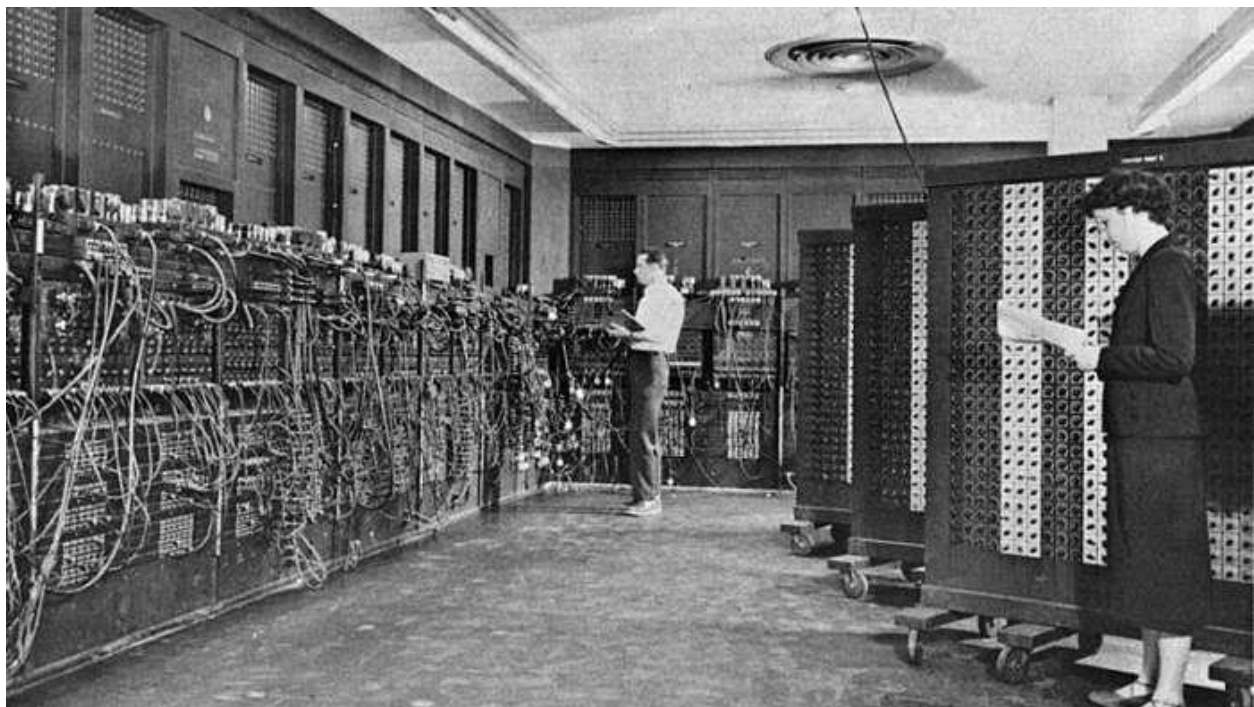


Fig 3:

The history of the hidden web is almost as old as the history of the internet itself. Obviously, the same technology that made the internet and the web possible, also makes the Dark Web possible thanks to its architecture and designs. Which is why it is fair to pin the start of the Dark Web to ARPANET. Which is the direct precursor to the internet of today? While ARPANET may not have had a Dark Web as we know it now from the start, it wouldn't take long before people started to make use of this technology for things they wanted to keep a secret. It turns out that the first ever online sale happened in the early 70s and was in fact cannabis. Students at Stanford sold weed to students at MIT, using ARPANET. Remember that at this point most people didn't have personal computers, much less home internet access.

The 1980s

In the 1980s, access to the internet for normal citizens is still a dream. This was the decade when everything needed for a worldwide web would fall into place. In the early 80s, the TCP/IP standard is solidified. By the mid- 80s personal computers and modems are, if not affordable, at least available for anyone to buy. Internet pioneers also invented the domain name system we use to resolve website names during this decade.

Data havens emerge as an idea at this time as well. Since the world was going global, worries about where data should be stored came to the fore. Storing your data in a haven meant sending it out of the country to a territory that had better legal protection against government spying. At the extreme, data havens would be in no country at all. They would be built on structures or vessels out in international waters. A similar idea to sea steading. Actual data havens in the 80s popped up in the Caribbean islands.



Fig 4:

The 1990s

The 1990s are without a doubt the time when the World Wide Web went mainstream. Thanks to web technologies like HTTP and FTP along with graphical computers capable of running a web browser, there was a sudden mainstream appeal to this whole internet thing.

Towards the end of the 1990s, there was a real leap in the technologies that allowed large amounts of data, such as multimedia, to be shared online. MP3 technology in particular led to a massive shakeup of the music industry. Thanks to the likes of Napster, people could perform illegal peer-to-peer exchanges of ripped and compressed music. This caused a complete meltdown among musicians and music executives. Lars Ulrich famously sued Napster which was really symbolic of the battle between old and new school. Today the music industry has adapted and streaming subscriptions are the norm. Without Dark Web like peer-to-peer exchanges it's doubtful we'd have the consumer-friendly online media world of today.



Fig 5:

The 2000s

The Dark Web proper really got its start in March of 2000 with the release of Freenet. The service still exists today and provides a censorship-resistant way to use the web. It is a true implementation of the Dark Web and provided a way for plenty of illegal information to pass around. This included illegal pornographic material and pirated content. Of course, actually exchanging money anonymously is still incredibly hard at this point, since you have to use cash. So Freenet doesn't lead to any black market activity to any significant degree.

A data haven called HavenCo was established in Sealand (a sea steading micro nation) which promised to store sensitive information in a place where no government could stick its nose. It seemed like a Dark Web dream, but by the early 2010s HavenCo was dead, dead, dead.

The most important Dark Web development of all time happened in 2002, with the release of TOR or The Onion Router. It was created by non-other than the US government, as a way to help their own operatives remain untraceable. It's no exaggeration to say that the Dark Web of today could not exist without this technology.

Late in the 2000s came the advent of cryptocurrency in the form of Bitcoin. The final piece of the puzzle needed to make the Dark Web really click.



Fig 6:

The 2010s



Fig 7:

The 2010s represent the era where cryptocurrency and TOR met to create the first proper black markets. The pioneer was the Silk Road, which is now long defunct. Despite taking all the important figures out behind the Silk Road, it has seemingly done little to stop the trade of drugs and other illegal goods and services over the Dark Web.

This is the era in which the Dark Web becomes a topic of public concern, rather than just something discussed at cyber security conferences. Many mainstream articles emerge that explain the difference between the massive Deep Web and the relatively tiny Dark Web. It becomes especially scary when it emerges that terrorists are using the Dark Web to communicate and coordinate. Ironical, given what the US created TOR for originally. Research published showing that the Dark Web is mainly being used to commit crimes.

Today

The Dark Web of today is reportedly in decline. Despite this, there is an incredible variety of hidden services and significant information exchange happening out of sight of the mainstream web. It doesn't really matter that the Dark Web is relatively small compared to the surface web as a whole. Its impact is disproportionately large. Small groups of hackers collaborating on the Dark Web can bring a multi-billion Dollar internet company to its knees. Hackers end up impacting millions of users. Dark net black markets are also thriving and putting both traditional and new synthetic drugs into the hands of anyone who wants them. Cryptocurrency has been the biggest factor in this maturation of the Dark Web.



Fig 8:

What the Future Holds

The technologies and methods that underpin the Dark Web are incredibly sophisticated. While most governments would prefer that something like the Dark Web didn't exist, they themselves need

technologies like encryption and onion routing for their own purposes. As long as powerful anonymization technologies exist and are effective, there will be some sort of Dark Web.

Whether the commercial, black market side of the hidden web has any future is a different question. While I have no doubt that Dark Web information exchanges will always be there, the future of black markets isn't that clear. It all hinges on cryptocurrency technology and whether it can be made anonymous in a secure way. While Bitcoin was at first thought to be untraceable, the authorities have figured out a few tricks to link specific transactions back to buyers. One stopgap has been Bitcoin tumblers. However, entirely new privacy-focused currencies such as Monero is the medium term solution.

Who will eventually win this arms race remains to be seen. There's little doubt that there will always be some sort of dark and hidden corner on the internet.

2.2 Dark Web & the Government

The dark web was actually created by the US government to allow spies to exchange information completely anonymously. US military researchers developed the technology, known as Tor (The Onion Router) in the mid-1990s and released it into the public domain for everyone to use. The reason was so that they could stay anonymous - it would be harder to distinguish the government's messages between spies if thousands of other people were using the same system for lots of different things. Tor now hosts roughly 30,000 hidden sites. It's called The Onion Router because it uses the technique of onion routing - making websites anonymous through layers of encryption. Most websites are also hosted on the .onion domain.

On April 11, Home Secretary Amber Rudd launched a multi-million pound cyber blitz on criminals selling guns on the dark web. She announced a £9million fund to ensure every police force in the UK has a dedicated cybercrime unit to bust its "sickening shopping list of services and products". The extra cash will tackle offenders who are exploiting the anonymity of the dark web - where users use freely available software to avoid being tracked - to trade in guns, drugs and child abuse images. This anonymity has attracted criminals seeking to avoid detection by law enforcement agencies

2.3 Who uses Dark Web & Why?

The dark web is used by all sorts of people for all sorts of reasons - but it's not surprising that it's used for illegal activity. A study by the University of Portsmouth in 2014 found that the most wanted type of content on Tor was child porn, followed by black markets for goods such as drugs, personal details and even guns. This type of site is regularly busted by police, who compromise them by distributing viruses and malware to users. The dark web is also used for hiding online activity related to finance, extremism, arms, hacking, abuse and fraud. However, for others the dark web has positive uses. For example, it can be used to avoid a national firewall, such as China, where users are normally blocked from accessing hidden sites. It can also be used as a tool for whistleblowing - infamous website WikiLeaks is hosted on the dark web, allowing whistleblowers to anonymously upload classified information to the press.

Do police ever catch people using the dark web?

Yes - although using the dark web makes it easier to evade detection but governments around the world are working to index, sort and catalogue the dark web as well as monitor it as much as they can. The UK government have a dedicated cybercrime unit to tackle the dark web with a focus on taking down serious

crime rings and child porn. Just earlier this year police caught Richard Huckle 'Britain's worst-ever pedophile' by secretly taking over a dark web site dedicated to child abuse.



Fig 9: Richard Huckle

Richard Huckle was handed 22 life sentences after pleading guilty to 71 child sex offences Credit: Getty Images The online network was made up of over 45,000 people who swapped sickening videos and images of children on a dark-web forum which was only accessible through a specially encrypted browser. Another take-down, called Operation Onymous, revealed over 400 "hidden services" in an effort by seventeen different countries coordinated by Europol and the FBI. The operation led to hundreds of pounds worth of Bitcoin being seized and 17 arrests - but only one person was identified and taken into custody.

Chloe Ayling Case

Chloe Ayling is a 20-year-old British model who was kidnapped by a notorious sex trafficking gang known as the 'Black Death Group' after being lured to Milan. The mother-of-one was held captive for six days in a remote Italian farmhouse after being led to Milan by fake promises of a photoshoot. She was drugged and stuffed inside a bag before being auctioned on the dark web. The Black Death Group is a shadowy online group which has been linked to multiple instances of kidnapping and people trafficking. Notorious on sections of the internet, it is claimed users of the dark web pay to buy women who have been abducted across Europe. Mum Chloe Ayling, 20, was driven to a remote farmhouse and held captive for six days after being abducted by masked men.

Ross Ulbricht

Ross Ulbricht was the man behind Silk Road, the internet's biggest market for illegal drugs - which was hosted on the dark web. Silk Road was reportedly worth \$34.5m and had nearly one million anonymous customers. On Silk Road you could buy drugs, services (such as hacking into Facebook accounts), pirated content, fake passports and more. You could even check the reviews and star ratings of each dealer left by other customers. Ulbricht was caught by the FBI in 2013, who shut down Silk Road and convicted him of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents and conspiracy to traffic narcotics in February 2015. He was sentenced to life in prison. Ulbricht will also be tried for procuring murder. FBI indictments claimed he ordered hitmen to kill people he thought would expose the identity of his clients. But investigators believe none of the six hits took place.

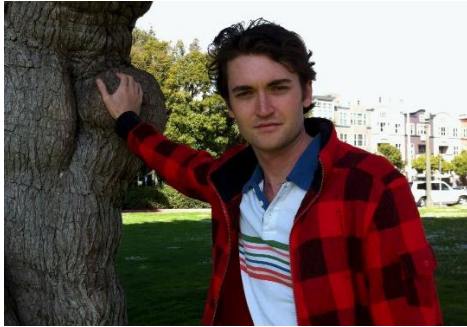


Fig 10: Ulbricht: the man behind dark web drugs emporium Silk Road

2.4 Is it illegal to access Dark Web? How safe it is?

There's plenty to see on the web, everything from the scores of your favorite sports teams to weather reports, reviews of the new French restaurant in town, and gossip from your friends and family members on social media platforms. But there's another world on the web that's mostly hidden from view and requires special browsers to access: the dark web. If that name sounds sinister, it's because the dark web encourages activity that people would rather hide from view. The dark web is where people can buy illegal drugs and firearms. It's also dotted with sites that specialize in illicit pornography, including child pornography. It's a part of the internet that you can't find with traditional search engines such as Google. Because it is hidden, getting to the dark web isn't easy. Most visitors first download Tor, or The Onion Router, a browser that allows users to search the internet anonymously. You can download this browser at torproject.org.

Finding specific sites on the dark web isn't easy, though. You have to know what you want. You can visit thehiddenwiki.org to see a list of dark web sites. Be careful when browsing that list, though. There are plenty of illegal sites on it. The dark web was created, then, for people interested in surfing the internet anonymously, and the sites within the dark web often cater to illegal activity. The question remains whether you are breaking the law by accessing the Dark Web.

The simple answer? The dark web itself is not illegal. What's illegal is some of the activity that occurs on the dark web. There are sites, for instance, that sell illegal drugs and others that allow you buy firearms illegally. There are also sites that distribute child pornography. The dark web itself, though, is not illegal. It offers plenty of sites that, while often objectionable, violate no laws. You can find, for instance, forums, blogs, and social media sites that cover a host of topics such as politics and sports which are not illegal. Using Tor to access and browse the dark web is not illegal. You will, though, have to be cautious. Surfing the dark web might not be illegal. But visiting certain sites, or making certain purchases, through the dark web is illegal. If you use the dark web to purchase illegal drugs or firearms, that's illegal. You won't be committing criminal acts, though, if you use the dark web to participate in forums or to read hidden blog posts anonymously. There are exceptions. You could potentially be participating in illegal behavior if you participate in certain forums, especially if it includes threats, hate speech, or inciting or encouraging criminal behavior. The key here is to use common sense. If something is illegal outside of the dark web, it will be illegal in this hidden section of the internet, too.

If you're careful, you can safely access and browse the dark web. First, download the Tor browser, which will give you access to dark web sites and keep you anonymous while searching the sometimes-seedier

corners of the internet. Tor will allow you to visit websites that have the .onion extension. That's why Tor's full name is The Onion Router. You might consider investing in a VPN, or virtual private network, too, when accessing and searching the dark web. A VPN helps keeps you anonymous when searching the internet, whether you are scanning the surface web or the dark web. When using a VPN, most likely only you and your VPN provider will know what sites you have visited. While it is legal to use a VPN in the U.S., it is always the user's responsibility to familiarize themselves with other countries' laws before using a VPN outside the U.S.

If you found your personal information on Dark Web

What if you find your own credit card, bank account, or other personal information on the dark web? What if you find sites selling your Social Security number or checking account number online?

Unfortunately, there's not much you can do to remove your information from the dark web once it's there. You should, of course, change the passwords you use to access your banking and credit card accounts. You might also want to update your login credentials to any services you subscribe to (like Amazon Prime, Netflix, or a meal delivery service, for example) and your healthcare and insurance accounts. You might also consider placing a credit freeze with each of the national credit bureaus, Experian, Equifax, and TransUnion. When you enable a credit freeze — which is free — you restrict access to your credit report which means lenders won't be able to pull your credit. This can help prevent thieves from opening new credit cards or taking out loans in your name. A credit freeze, though, cannot stop all criminal activity. If identity thieves have gained access to your credit card account, for instance, they can still use your card to make fraudulent purchases.

You should also order your credit reports from Experian, Equifax, and TransUnion. You are entitled to one free copy of each of your three reports once a year. You can order your reports from AnnualCreditReport.com. Once you do, study these reports for anything unfamiliar or unusual. If your reports list a credit card account under your name that you don't remember opening, that might be a sign that thieves have used your personal information to sign up for a card in your name. Call that credit card provider and tell them that you never opened the account. If you suspect that you have been the victim of identity theft, file a report with the Federal Trade Commission [here](#). Next, contact the companies at which the fraud occurred — usually your bank or credit card providers. Inform each of the three major credit bureaus, too.

Finally, consider investing in a credit-monitoring service that can alert you whenever potentially suspicious activity occurs on one of your financial accounts. This type of monitoring could help you catch identity theft before extensive damage is done. You might consider signing up for Norton 360 with Lifelock, which provides identity theft protection, device security, and online privacy — all of which can be helpful in protecting your information from being accessed.

3 Dark Web E-Commerce

3.1 Kind of businesses are done on Dark Web

The Dark Web has a pretty terrible reputation as a place where criminals and other undesirables congregate for nefarious purposes. While it is true that illegal (or at least frowned upon) activities are rife

on the Dark Web, that's not the whole story. There are actually plenty of things to do on the Dark Web that won't get you in any sort of legal trouble. The Dark Web is also a haven for people who want the true privacy the internet has always promised. Remember, simply accessing the Dark Web is not a crime. It's no different from accessing any surface website in that sense. It's what you do on Dark Web and the sort of content that you consume that has the potential to get you into trouble.

For the Book Lovers

For lovers of all things written down, the Dark Web offers some compelling content. Two prominent sites worth mentioning are the Imperial Library of Trantor and Jotunbane's Reading Club.

Imperial Library of Trantor - One of the best deep web links for book lovers. If you love to read deep web books, then you must bookmark this dark web site. They have a vast collection of different category books like fiction, crime, general, mystery, computer etc. Yes, they have almost every category book in their database. As they claim they have 116174 books. This dark web book link also has forum section, you can join them to discuss about books with other forum members. If you want to know what's the new at Imperial Library of Trantor then you can visit their News section. You can simply search your favorite book by typing in search box. Home page is well designed. You will find Last books added Most visited books and most download books at home page. If you want to read or download the book, just click at book image. You will find two options here, one for read and second for download. You don't need to look further if you have this dark web link.

Comics Book Library - If you are in mood of reading Comics, this hidden web link can be your favorite place. Currently, they have 1201 comics. They have categorized their collection in a standard way for your ease. You can read or short Comic by Title, Comic by Year, Comic by Publishers, Comic by Scanner, recently Added, and Random comic etc. I must say this is the best place at dark web for comic lovers.

Clockwise Libraries - This dark web book link has very vast collection of books. Don't be confuse they don't offer their collection at home page. To see their books collection, you need to click given book image and you will get their hidden collection of amazing books. They have organized their database in very friendly way. I really like it. They categorized as Alphabetical index of the 48448 authors, the 2293 series, 5127 publishers, 15367 tags, 9 ratings, 25 languages, 51469 books, 50 most recent books. You could take an idea of these records how large collection they have!

ParaZite - Parazite has huge collection of secret papers and files. You can access these secret documents by visiting given onion link. Main categories they cover are Documentaries, Porn, History, Weapon, Hacking, etc. This dark web link has some illegal stuff like drugs related research paper, CP documents and much more. If you are interested in know such type stuff, then visit the website.

These are only some of the websites that will provides you unlimited amount of E-Books. There are hundreds of websites to get E-Books. Now, it is illegal to get access to pirated, copyrighted material. Just so you know. However, it's perfectly fine to join these communities in order to discuss the books themselves with like-minded lovers of literature. So popular is the Dark Web among serious literary aficionados that the Dark Web has its own exclusive literary magazine. It's called The Torist and it is deadly serious. You'll find short stories, poems, essays and more.

Various Clubs

The Dark Web is littered with special interest sites and forums. Just about any niche activity, you can think of, there is probably an elite, exclusive or just plain weird group of people who get together for the love of it.

For example, “TheChess” is a place where Chess fanatics can play online and also while away the hours arguing about which opening is really the best. I’ve also already mentioned book clubs above. They are so big on the Dark Web they deserved their own section.

There are also forums like the Intel Exchange, where you can get information both offensive and extreme, along with more mundane fare. Like a good conspiracy theory? You’ll find plenty here. Along with discussions on things that are considered taboo in many societies. However, talking about taboo things is perfectly legal. Now you can sate your curiosity in true privacy.

Journalism

One of the noblest legitimate uses of the Dark Web is putting journalists in touch with people who must get their story out, but can’t afford to do it publicly. It turns out that the flip-side of this use case is also quite welcome on the hidden part of the net.

“ProPublica” is at the spearhead of this. It’s a publication which has decided to publish stories on an official Tor site so that readers can access the content with complete anonymity. This deals a deathblow to regimes that don’t allow their citizens to read whatever they like. It’s one of the best reasons to support the existence of the Dark Web. Now, I know that to the people who need to access journalism via the Dark Web are probably breaking laws in their home countries. However in the rest of the free world simply reading an article other people don’t like can never be a crime.

Search Engines

Search engines almost literally make the Web work. Without them, you could never find a site unless you had its exact address. Unfortunately, search engines like Google track you across the web. They sell your information and target adverts directly at you. For many people, it’s a fair trade-off given how useful the search algorithm is. However, on the Dark Web, you can get those same search results from the surface web without the possibility of the search engine knowing who you are in the first place.

Many of these privacy search engines are also on the surface web. DuckDuckGo, for example, has both a normal URL and a DuckDuckGo onion site. While using a search engine like DuckDuckGo is already pretty darn private on the surface web, using via Tor means no one will even know you visited DuckDuckGo in the first place. Avoiding the whole guilt by association issue.

Cryptocurrency Services

Cryptocurrency is essential to the Dark Web since it is used to facilitate black market transactions. However, just like the Dark Web itself, Bitcoin isn’t illegal by itself.

There is however a problem with Bitcoin when it comes to privacy. It turns out that Bitcoin is quite traceable under the right circumstances. Bitcoin uses a public ledger after all. This also means that Bitcoin you have been paid with can be tainted with ones that have been used for illegal purposes before. New cryptocurrencies like Monero have been developed to solve the issue, but Bitcoin is still the most widely

accepted. Coin tumblers mix up and slice your Bitcoins so that it becomes much, much harder to trace them. It's a good way to cleanse your Bitcoin from things that have nothing to do with you.

Tumblers aren't the only Dark Web cryptocurrency services on offer. You can also find exchanges and wallets in the depths of the Dark Web. Just be very careful of being scammed. As long as you don't use your Bitcoin to buy illegal things, using Dark Web Bitcoin services should be perfectly legal.

Scientific Papers & Journals

Believe it or not, it's actually pretty hard to get your hands on the latest scientific papers. Journals charge an insane amount of money for research papers, none of which goes to the researchers, who would happily give the papers away for free. The rise of Open Access journals has helped a lot, but there is still a significant barrier for public access to direct scientific research. So most people have to get their science news through the lens of popular publications or public science writing. The average person may not care, but it does make life hard for people who don't have the luxury of a university or corporate research accounts with the likes of Elsevier.

The Dark Web has risen to the occasion, with sites such as Sci-Hub offering access to thousands of papers that are usually behind academic paywalls. Now, depending on where you live this is in a legal grey area. So you might want to Google (or DuckDuckGo) the legality of Sci-Hub in your region, but one way or another it's an amazing resource. It works by crawling university databases and other deep web resources looking for papers people have requested. At last count, the total number of papers was climbing steadily to the 50 million mark. That's incredible.

It's not the only game in town either. For example, there's also the American Journal of Freestanding Research Psychology. Although this is actually meant as a Dark Web psychology journal.

Social Media

Social Media websites are getting popular because of the growth of concerns about privacy of users. Social media still has a place in the online world. Plenty of people enjoy the simple act of sharing and interacting. However, the big social media platforms like Facebook don't let you use an anonymous identity. For example, Facebook has a dark net site which is used by over a million individuals every month. Several Dark Web alternatives to Facebook have popped up over the years. Blackbook and Torbook are common examples, although sites using those names come and go. Such sites are designed to look and feel like Facebook. You sign up with a fake or isolated email address and set up an anonymous profile. Obviously, you should not put any personally identifiable content on these sites.

Ironically enough, there is a Facebook onion address. It's useful for people who want to access Facebook without their governments knowing, but you're still subject to their real name policies. So make of that what you will.

Cybersecurity

There are certain advantages to the enterprise in being able to use the dark net for enhancing network and customer security. There is a wealth of information on dark net forums which can alert cybersecurity teams about potential vulnerabilities or emerging threats. Advanced intelligence on new hacks that are being used against them, or knowledge of tools like botnets or compromised servers, can offer enterprises significant cost savings when developing their cybersecurity methods. Active involvement in monitoring

dark net activity can also be extremely useful in guarding against phishing attacks, for example, or when customer data has been breached and appears for sale on the dark net.

Secure Communication

The prospect of secure communication can be attractive to news organizations who can use it to communicate with their sources. As a result, investigative reporting organizations like ProPublica (<https://www.propublica.org/>) now have their own dark net sites. And there is also an increasing use of the dark net by other types of institutions, like the UN, which uses it to monitor activity that it shares with the police and governmental groups.

ProPublica – ProPublica was the first major news organization to launch a version of its site on the dark web, catering to readers who need or prefer to stay anonymous online. As Wired reports, the publication launched as a "hidden service" on the Tor anonymity network on Wednesday, guaranteeing readers that internet service providers or other snoops won't even be able to see that they've visited the site.

Users could always anonymously access ProPublica through a Tor browser, but not all of the publication's pages are protected with SSL encryption, leaving open the possibility that eavesdroppers could see what content they look at. Even if a user doesn't visit a non-encrypted ProPublica page, others could still see that they had visited the site. Operating as a hidden service negates those risks, the news outlet says. Tor hidden services mask a website's IP address, and can only be used when running Tor software.

Business Intelligence

One of the original functions of the Tor network as a government-sponsored initiative, was to ensure secure communications. As such, the dark net has arguably always been an ideal medium for the gathering and sharing of intelligence. It is hardly surprising that enterprises have also begun to see some competitive advantages in using the dark net in this way. There is a vast range of data on the dark net – so-called 'dark data' – which enterprises can use to develop customer insights, such as better understanding of consumer preferences. Dark net data can also be mined to refine operational, marketing, and new product insights. Enterprises can gather this intelligence themselves, but increasingly there is a developing industry that provides dark net information to the enterprise.

Credit Monitoring

Several credit rating firms, like Experian38, already offer services for customers to check if their details (SSN, phone number, ID info) are on the dark web. This suggests there is the potential for lenders or other credit agencies to build in extra safeguards when underwriting loans, by acquiring insights from the dark net when looking into the credit history of applicants.

Recruitments

There is also evidence that some enterprises are making use of the dark net as a tool for recruitment as it provides a novel way of reaching a community that is potentially out of reach to traditional recruitment agencies. One example was the campaign run by an anonymous organization calling itself Cicada 3301, which posted a series of complex puzzles that eventually took candidates into the dark net. The identity of the organization remains mysterious, but there are obvious precedents here for imaginative recruitment. When combined with the kind of enhanced intelligence about job candidates offered by the

dark net, it seems clear that HR and job recruitment is one of many aspects of business operations likely to evolve as use of the dark net develops.

Intel Exchange

The Intel exchange is pretty much what you'd expect based on the name. It's a place where people come and exchange "intel" in the "intelligence" sense of the word. Valuable information in all manner of topic areas. People share information here that you wouldn't normally expect. A lot of it is of course just crazy and untrue. Plenty of conspiracy stuff and the like. So basically like Wikipedia, but with even less vetting. The range of topics is impressive. Supposedly suppressed technologies get discussed in its own sub-forum. People provide insider info about current events or things related to current events.

There are also more mainstream topics such as computer hardware, software, mathematics and more. Read the Intel Exchange at your own risk, but it's sure to be a fascinating experience.

3.2 Demography

According to the statistics of Statista, in 2019, 12% users from the total users of internet worldwide have used some technologies that allows access to the dark web.

A screenshot is given on the next page from the statistics made by statista:

As we can see, India is topping the list with a number of users of 26% of total users who have access to the dark web. And other countries are listed below with percentage:

- Russia 22%
- Brazil 21%
- Indonesia 20%
- Turkey 16%
- South Africa 16%
- Sweden 16%
- Mexico 13%
- Korea 12%
- Poland 12%

And so on.

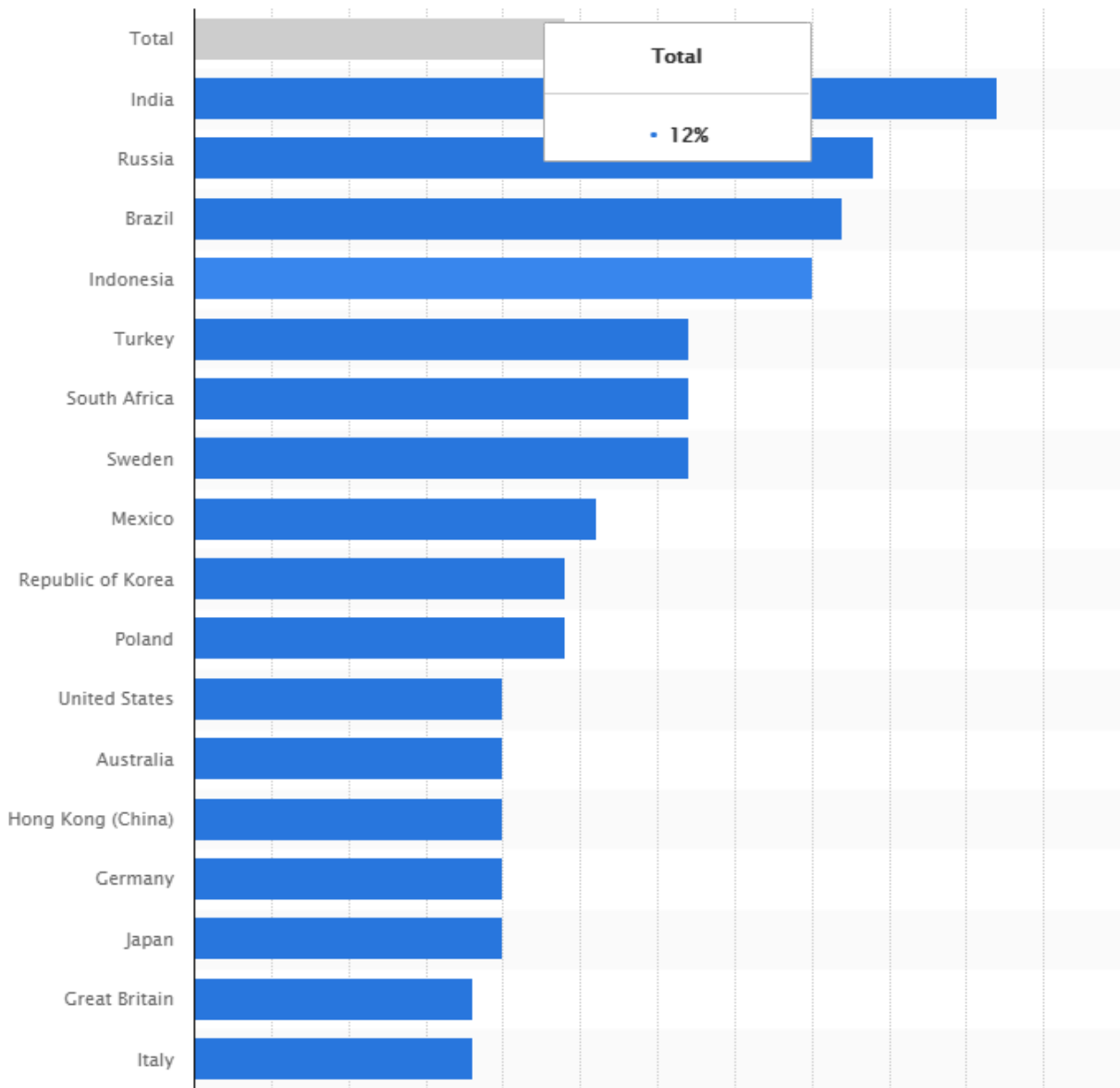


Fig 11: Percentage of User access into Dark Web

Some Statistics & Facts

At least 100 darknet marketplaces were active 2019: Darknet marketplaces are where one can find everything ranging from marijuana to rocket launchers. There would be sellers offering credit card info and email IDs too. Human trafficking is often associated with these marketplaces, as well. Authorities around the world are trying to shut down these marketplaces and have done so successfully on many occasions. However, new marketplaces are cropping up at a higher pace on the Dark Web, and there is always a cat and mouse chase between the authorities and marketplaces.

The Dark Web made FBI the second-largest owner of Bitcoins: As the authorities cracked down the operations of Silk Road, the subsequently confiscated a lot of bitcoins from various accounts of Ulbricht. They got 144,000 bitcoins from Ulbricht's rented servers in Iceland. FBI has still done nothing of these bitcoins, and their current aggregate value is around \$1.2 billion. It will be interesting to know how FBI plans to deal with all those digital assets.

Information from 620 million accounts was available for sale on the dark web: We often come across the news of hackers getting into website servers and stealing away account information of millions of users. If you ever wondered, what would one do with these millions of accounts, then selling them is one of the answers. And, no points for guessing it right, hackers come to dark web to sell such data. A report showed that account information stolen from 16 websites, making up for 620 million user accounts, was on sale on the dark net. Not all the compromised websites knew that their servers were breached. All the data was mined over one year, and at least one person bought it.

The job opportunities on the dark web: You never know what you may find on this part of the internet. There was once a job posting that said one could earn \$255k on serving for six months. The job description had nothing much to give user an idea of what's going on. All it mentioned was that it was a six months job, the person would stay out of communication, and the one applying for the job should have some combat experience. One can only wonder what kind of job it can be.

Bitcoin helps this digital black market survive and thrive: You already know that dark web provides all kinds of things and services that one can possible thing of getting. Marketplaces on dark net perform in a way similar to one on surface web. Since identities are often masked, sellers often maintain the same alias. Buyers leave reviews of stuff they buy on such places, and it is these reviews that help other buyers to know if they can trust a seller. Reviews are of utmost importance on such forums. The one thing which is at the foundation of such a huge business is cryptocurrency.

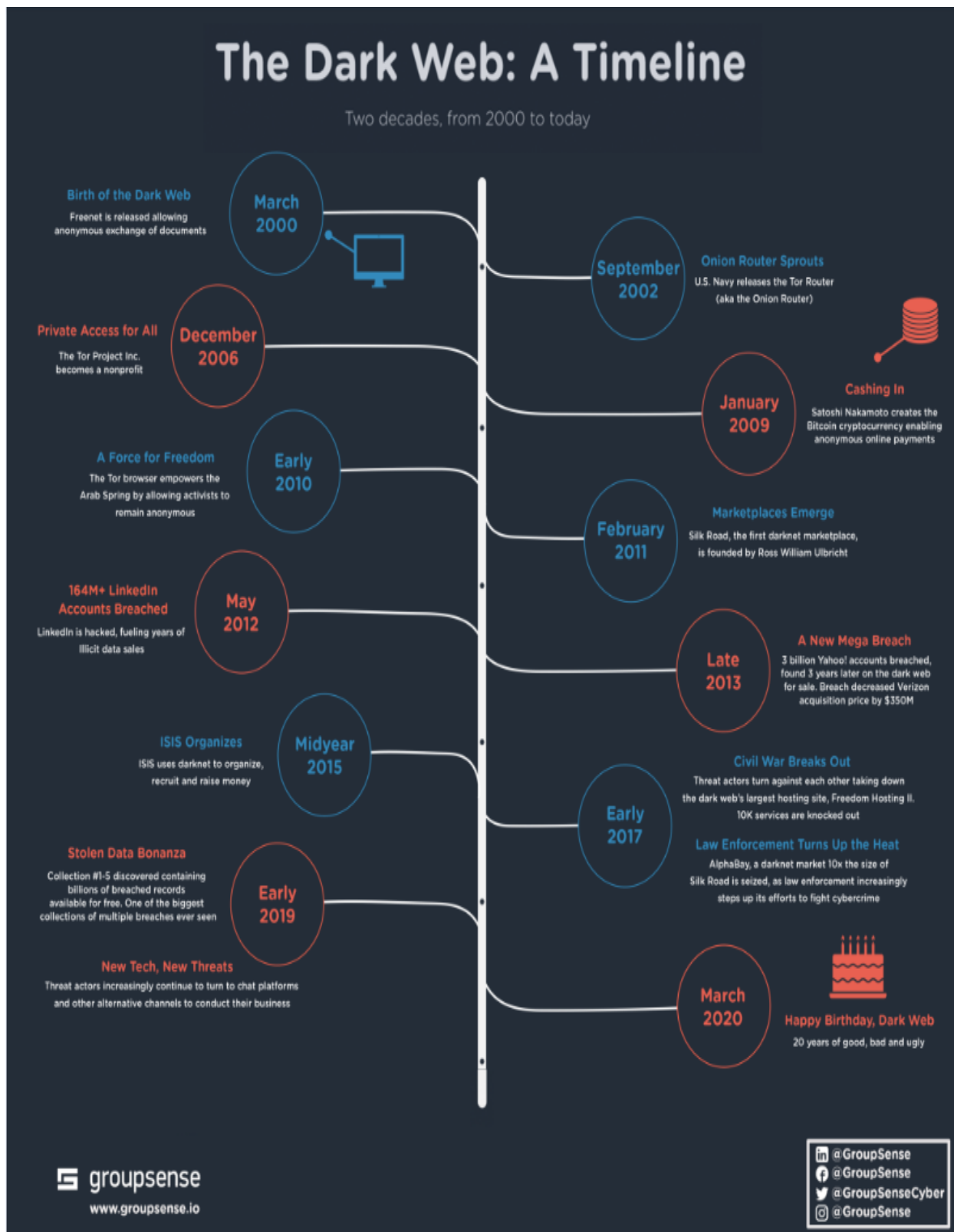


Fig 12: A timeline of Dark Web

3.3 Stories/Anecdotes from Dark Web E-commerce

Wish Pills: One person found "wish pill" on a darknet market. Here is the description – Basically you take the pill, make a wish and it's supposed to make it come true. It just made me laugh how much they were trying to sell it off as something real, they made up fake elements that were supposedly found in nature and showed videos of them "making the pill" (Which was really just a bunch of blue lights being flashed at the screen). They were selling it for a \$100 a pill, sad thing is there were probably a few idiots who actually bought it.

The whole horn: Sometimes you may need something specific and you have nowhere else to turn. If that's the case watch out for a steep price tag. This Redditor explains – “A few years ago I went searching for rhino horn for a story, one guy said he had a couple of whole horns he'd sell for six figures. I had to pass.”

A mind-blowing experience: Surprises are often in store. And so are vendors with senses of humor. As is showcased with this story – Silk Road. Circa 2013. Purchased what was promised as a "mind-blowing" experience. Received a Dust Buster two days later. Strangely, no complaints on my end.

Survival guide for prison: From Quora – There was an interesting PDF with easily 1,000 pages written by ex-inmates about how to survive in prison, how to get drugs in and out of prisons, gangs etc.

Don't forget the simple things: And sometimes people are selling things you didn't even know you needed to buy online, like carrots or pretzels. There was a German man selling pretzels, just pretzels.

Most of the deep web isn't accessible: One Reddit user explained that most things on the deep web simply aren't visible to the average person — they're hidden behind passwords or aren't linked to on any other websites. Most things that are visible on the deep web are visible because someone wants them to be. Everything else generally isn't easily accessible.

Mariana's Web: This is one of the most uncertain dark web stories out there. Mariana Web is a supposed hidden site with information on secrets about the earth. The site is named after Mariana's Trench, the deepest point on earth because Mariana's web is buried very deep even on the deep web. It is believed that this site exists even though there is very little evidence to show that. The site is reported to contain information about communication with other life forms, the location Atlantis, and a subset of the internet used extra-terrestrial beings to monitor us.

Anonymous \$255,000 Job: Some deep web stories have very few incentives to attract people but this particular one promises people \$255,000. Aside from the fact that being a job listing on the dark web makes this a scary offer, the job description is extremely ambiguous offering only the points listed below as what is needed for the job.

- Combat experience
- 6 months on a ship
- No communication with the outside world
- \$255k is the total payment for 6 months

Five Guys: According to a Reddit post, "Was on Tor, browsing da usuals. Go out to eat foods at the Five Guys. Come back. More Tor. Find a picture of me eating at Five Guys.”

Mysterious Logins: This isn't so much a single story, but more of a mystery from the Dark Web itself. While most hidden services on Tor are actually pretty easy to find thanks to links on the clear web, not everyone is so welcoming. There are numerous sites on Tor that are a complete mystery. If you visit them you'll just see a nondescript login page. There's not even a tiny clue as to what sort of sites lie behind these stony digital walls. It could be a cult, the FBI or something too horrible to imagine. All we can do is pretend they don't exist or become obsessed with these mysteriously locked doors to some sort of even darker web.

3.4 Market Comparison Chart

Dream Market

ITEM TYPE	DETAILED STATS
Name	Dream Market
Established	Nov-15-2013
Main url	http://wet4o7ali46htxkm.onion/
Support Multisig	⊗
Security Issues	😊
Active Warnings	None
2 Factor Authentication	☑
Finalize Early	Allowed
Commission	4%
Vendor Bond	0.1 Btc
Forced Vendor Pgp	Yes
Total Listings	0
Business volume (weekly)	0.00\$
Current Status	Shutting Down on April-30-2019

Fig 13: Dream Market

Empire Market

ITEM TYPE	DETAILED STATS
Name	Empire Market
Established	Around April-2018
Main url	Oaj4azj6wtxhlojk.onion
Support Multisig	<input checked="" type="checkbox"/>
Security Issues	😊
Active Warnings	None
2 Factor Authentication	<input checked="" type="checkbox"/>
Finalize Early	<input checked="" type="checkbox"/>
Commission	4%
Vendor Bond	\$500
Forced Vendor Pgp	Yes
Total Listings	52.7k (as of Apr 2020)
Business volume (weekly)	\$1.1 Million Per Week (estimated)
Current Status	Active

Fig 14: Empire Market

Big Blue Market

ITEM TYPE	DETAILED STATS
Name	Big Blue Market
Established	Aug-25-2019
Main url	bigblueonef5sf26.onion
Support Multisig	⊗
Security Issues	😊
Active Warnings	None
2 Factor Authentication	<input checked="" type="checkbox"/>
Finalize Early	Allowed
Commission	1.5% to 3.5 %
Vendor Bond	\$250 / \$150 / \$0
Forced Vendor Pgp	Yes
Total Listings	6300 (as of Apr 2020)
Business volume (weekly)	N/A
Current Status	Active

Fig 15: Big Blue Market

Agartha Market

ITEM TYPE	DETAILED STATS
Name	Agartha Market
Established	Around Mar/Apr 2019
Main url	http://agarthaourmnyhq3.onion
Support Multisig	<input checked="" type="checkbox"/>
Security Issues	😊
Active Warnings	None
2 Factor Authentication	<input checked="" type="checkbox"/>
Finalize Early	Allowed
Commission	4%
Vendor Bond	0.04 Btc
Forced Vendor Pgp	Yes
Total Listings	60k Scraped Listings (Not real)
Business volume (weekly)	N/A
Current Status	UP & SCAMMING

Fig 16: Agartha Market

Yellow Brick Market

ITEM TYPE	DETAILED STATS
Name	Yellow Brick Market
Established	Around April-2019
Main url	http://7wxzaxsqibuinpyc3muazc374glv32ve73jw6zf7q6bqtc4mfynsjyd.onion
Support Multisig	⊗
Security Issues	😊
Active Warnings	None
2 Factor Authentication	<input checked="" type="checkbox"/>
Finalize Early	Allowed
Commission	4%
Vendor Bond	0.03 BTC
Forced Vendor Pgp	Yes
Total Listings	900 (As of Aug 2019)
Business volume (weekly)	N/A
Current Status	Active

Fig 17: Yellow Brick Market

3.5 How Dark Web Markets Are Exploiting the Coronavirus Pandemic

At Elliptic, their data team work constantly to gather the latest intelligence on the illicit use of crypto-assets. Key to this is monitoring the rapidly-evolving use of dark net markets, e-commerce platforms that facilitate the trade of various illicit goods and services. Vendors on these sites can post listings for everything from narcotics to stolen credit cards and hacking tools, with payment accepted exclusively in crypto-assets.

These vendors are opportunistic, jumping on any opportunity to supply goods that are difficult to obtain elsewhere. Over the past few weeks they have begun to exploit the opportunities presented by the coronavirus pandemic.

Masks

Hundreds of listings have recently appeared on dark net markets for N95 respirator masks. Usually priced at less than \$1 each, these masks have been in very short supply and their sale for non-medical use has been restricted. The listings shown below offer N95s in bulk at around \$1.75 per mask - a surprisingly low mark-up on retail prices. Compare this to the prices charged by vendors on legitimate marketplaces such as Amazon or eBay, where N95 masks have been listed for sale for upwards of \$10 each.



Two listings offering bulk N95 masks for purchase, on a darknet market site

Fig 18: N95 masks on sale

Of course with all dark net market listings posted by pseudonymous vendors, there is a chance that they are fraudulent, and that buyers don't end up getting what they paid for. Marketplaces therefore employ vendor reputation systems so that buyers can review their purchases and provide useful insights to future buyers. Few reviews have been posted for masks, due to the short period of time that they have been on sale. However what this does reveal is that many of the mask vendors are established, well-reviewed sellers. Many have previously sold narcotics and other illicit goods and services, and have now turned to masks as an additional revenue stream.

Beyond the usual dark marketplaces, a new online shop has launched - dedicated to the sale of masks. The operator of this site claims to be a European wholesaler for hospitals, but believes that "Everybody need a chance to get a Mask for protection - Not only medical employees!"



A dedicated darknet site offering N95 masks for sale

Fig 19: A dedicated dark net site offering N95 for sale

Diagnostics

Another critical shortage during the epidemic has been for coronavirus diagnostics. The lack of widespread testing capabilities has been cited as a key reason why certain countries have been particularly hard-hit. And so dark net market vendors have once again stepped in to exploit the opportunity. The listing below offers “COVID-19 test strips”, starting at \$92 each.

Operation Instructions

Correct use, convenient and quick

1. Constant Temperature and Static position;

2. Massage finger pulp;

3. Disinfect with alcohol tablet;

4. Blood sampling and acupuncture into the abdomen of fingers ;

5. Wipe off the first drop of blood with sterile dry cotton ball;

6. Use disposable micro pipette to suck blood;

7. Added blood drops to the test card ;

8. Add diluent and start timing ;

9. Allow to stand for 20 minutes to read the result .

COVID-19 test strips diagnostic kit for Self-test CORONAVIRUS

Quality rate:

Type: Physical

Offers

- 63.88 \$ per item, for at least 500 products
- 70.38 \$ per item, for at least 250 products
- 74.71 \$ per item, for at least 100 products
- 81.2 \$ per item, for at least 50 products
- 86.62 \$ per item, for at least 25 products
- 92.03 \$ per item, for at least 10 products

Coronavirus tests for sale on a darknet market

Fig 20: Coronavirus tests for sale


Coronavirus “Cures”

The pandemic has of course created huge interest in potential COVID-19 treatments, with a number of therapeutics and vaccines in development. However none have yet to be proved effective.

However there has been anecdotal evidence that existing drugs such as chloroquine, a malaria treatment, could be an effective treatment for COVID-19. Public interest in this drug has been sparked by repeated

comments from US President Donald Trump about the drug's potential, despite the absence of regulatory approval for its use.

And so we have started to see listings for chloroquine on dark net markets. The listing below refers to the claims made by Donald Trump, and offers a pack of 150 pills for \$500.



chloroquine it kill Coronavirus 150pils
Coronavirus and chloroquine: Has its use been approved in ... [www.bbc.com](#) - news President Trump claims a drug used against ...

Sold by **hennessy12** - 1 sold since March 22, 2020 **Vendor Level 1** **Trust level 1**

	Features		Features
Product Class	Physical Package	Origin Country	United States
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

DHL - 7 days - USD + 40.00 / order


Purchase price: **USD 500.00**

Qty: 1 **Buy Now** **Queue**

A listing for Chloroquine - referring to claims made by Donald Trump

Fig 21: A listing for Chloroquine

Get the cure Vaccine for Coronavirus



Sold by: **kinghacks** (1) (5/5 ★)
Trust level: **Level 1**
[Send Message to kinghacks](#)
[Add to favorites](#)

Product Type: Physical
Payment Type: Escrow
Shipping Options
DHL - 5 Days - \$30.00

Quantity
1

Buy for \$15,000.00

A listing for a coronavirus "cure"

Fig 22: Another Listing

Narcotics

For the majority of darknet market vendors it will be business as usual during this global pandemic. In fact as for other online retailers it presents a unique opportunity, and may herald a further shift towards online commerce. Many darknet narcotics purchasers will now be largely confined to their homes, with more free time and fewer opportunities for face-to-face transactions.

Many vendors are using the situation as a marketing opportunity, offering "Coronavirus discounts" or "COVID-19 end of the world special offers". The listing shown below is for a "Corona Lockdown Survival Pack" The contents? Cannabis and toilet paper.

Coronavirus hits dark net revenues & crypto gambling craps out

The Chainalysis report suggests that dark net markets have suffered substantial declines in revenue following the recent drop in Bitcoin's value. That's despite the 70% increase in dark net purchases made with bitcoin in 2019 compared to 2018 that Chainalysis reported in January. This downturn is unusual because, at least in the past, activity on these platforms was largely unaffected by market volatility—with BTC being used to buy drugs, firearms, and stolen credit card data irrespective of how much the cryptocurrency was worth. Granted, there are other factors at play here. The pandemic has affected freedom of movement and global supply chains. This has undoubtedly affected the supply of popular substances such as fentanyl—and it's no coincidence that large volumes of this drug were manufactured in China's Hubei province, where the pandemic began. "Perhaps dark net market customers aren't buying as many drugs given the public health crisis. It's also possible that vendors slowed down sales during the price drop, out of fear that the Bitcoin they accept one day could be worthless the next," the Chainalysis report notes.

It may be fashionable to assume that crypto-based gambling services would have been a big winner during the COVID-19 pandemic, but the Chainalysis research suggests an uptick in demand hasn't been forthcoming. Volumes of bitcoin flowing into online casinos and gaming sites have been on the decline since March 9— despite many people being stuck at home, it seems few have opted to have a flutter. The lackluster performance of the gambling sector may not have anything to do with bitcoin's price, however. Chainalysis says there has long been a weak link between the gambling sector's revenue and BTC's value. This basically means that many gamblers would use BTC to place a bet even if the cryptocurrency was at an all-time high, because they "don't approach gambling rationally or with an expectation of profit, but rather as a way to have fun."

Good News for Legitimate E-Commerce

On the other hand, online and even (still open) brick-and-mortar merchants providing legitimate goods and services that can accept bitcoin—such as AT&T, Microsoft, game streaming platform Twitch and, indirectly, Amazon—have not met with a fall in purchasing volumes they would have normally expected with bitcoin's declining value, Chainalysis said.

The company provided a few theories as to what might have shielded merchant services from bigger falls. For one thing, it's possible that cryptocurrency users are opting to buy essential items through these platforms—products that aren't currently available from outlets that accept fiat.

For another, demand for merchant services might have enjoyed an uptick because local retailers have had to close because of COVID-19. Finally, recurring payments, such as subscriptions for web hosting, might also be keeping revenues steady as other income streams dry up.

Warning that this is no ordinary Bitcoin price drop, the Chainalysis report added: "It's a one-of-a-kind market event brought on by an unprecedented public health crisis. The question for cryptocurrency businesses is whether or not they'll be able to return to their previous transaction levels and if their customers' usage patterns will return to normal."

Note: All the information are taken from an article of [elliptic.co](https://www.elliptic.co)

3.6 Dark Web & Surface Web Search Engine Index

Dark web search engines exist, but even the best are challenged to keep up with the constantly shifting landscape. The experience is reminiscent of searching the web in the late 1990s. Even one of the best search engines, called Grams, returns results that are repetitive and often irrelevant to the query. Link lists like The Hidden Wiki are another option, but even indices also return a frustrating number of timed-out connections and 404 errors. Many so-called Dark Web search engines are really just repositories of links. This is actually how early search engines on the internet worked. More like a giant phone book than a web crawler that indexed the contents of sites. Then, of course, there are search engines on the Dark Web that search the surface web. In other words, they provide a super-secure way to search for things on the regular internet that you don't want to be attached to your history or identity. So adjust your expectations a little of what it means for something on the Dark Web to be a search engine and feast your eyes on these excellent Dark Web destinations, in your search for hidden network content.

When we search about something on any search engine, it simply displays up a few results consisting of about 10 links and we found at least one link to satisfy our searched term most of the times. This is called as simple searching or we may call it web surfing. This way we are simply surfing over the web pages using a traditional search engine. But what is exactly meant by Deep Web Search? To explain this, we are going to take help of illustrative examples. We use the Internet, means the Web to explore, learn and find a lot of things. These things include the information gathering, photos and videos gathering, documents gathering etc.

When one makes use of Internet to find anything, there are two types of methods that may be used under our today's scenario. The very first method is to find the relevant information by searching through the Search Engine like Google and then afterwards surfing the web in a simple way. The next method is the Deep Web Search which is not known to most of us. Deep Web Search is to browse the web in an advanced way to find a kind of hidden information or any other kind of data which we cannot find by simply browsing the web using the search engines. It may also be said that Deep Web means to explore the hidden Internet.

Most of the people think that using a search engine like Google, they may find some relevant information and hence also get satisfied but actually, they don't know the Internet is not just limited to it. Sometimes, we come across some websites which are themselves a search engine such as the collection database sites.

What is Hidden Web Search Engines?

Both Deep web & Dark Web refers to Hidden Web search engine. The terms "deep web" and "dark web" are often interchangeably used although they are not the same thing. The dark web is technically a small sliver of the deep web, which accounts for 0.01 percent, but the horror stories you hear about the dark web do not actually occur on the deep web. In fact, the majority of the content on the deep web is very similar to the content found on Google, the surface web. And without knowing it, we use it every day.

What is Deep Web Search Engine?

Now coming to understand the meaning of Deep Web from the words itself. The word "Deep" clears and exclaims as the web which is deeply hidden in the depths of web. There may be a lot of reasons why

search engines do not index these kind of information in the search engine. There might be the factors like the owners of the deep web content may not like to display up their content publically via the search engines and so on more. Anyhow, we are going to learn now about Deep Web Search Engine in Detail.

Deep Web is the data that is not indexed by a standard search engine like Google or Yahoo. The Deep Web refers to all web pages that search engines cannot find, such as user databases, web forums required for registration, webmail pages and pay wall pages. Then there's the Dark Web or the Dark Net—a special part of the Deep Web hidden. The Deep Web and the Dark Web are the fascinating subjects for the Netizens. However, when you hear the term 'Deep Web' or 'Dark Web,' you usually classify it into one. If yes, you're mistaken.

There are also different types of Deep Web Search Engines to research or simply search about different type of contents. Some Deep Web Search engines are meant to simply found the deep web textual content and some to find deep web media content. According to some source, the size and the volume of content of the Deep Web is much more than the normal web which browse in general from day to day. But why we are unable to find this kind of web information? The simple answer it is deeply packed, protected or even hacked.

What is DARK WEB Search Engine?

Dark Web is where you can operate without tracking, keeping you completely anonymous. The Dark Web is much smaller than the Deep Web and consists of all sorts of websites selling drugs, weapons, and even hiring murderers. These are hidden networks that prevent their presence on the surface web and their URLs are tailored to (.onion). These [website name].onion domains are not indexed by regular search engines, so you can only access Dark Web with special software-called the TOR. TOR is free, and downloadable by anyone. Many of us heard about the Dark Web when the largest underground online marketplace on the Silk Road was dismantled after an investigation by the federal authorities in the United States. But what if you can still dig in your regular browsers the Darknet content without the need for TOR?

Why isn't Google's deep web search available?

Google does not provide deep web content primarily because this content is not indexed in regular search engines. These search engines therefore do not show results or scroll to a document or file that is not indexed on the worldwide website.

The content is supported by HTML forms. Regular search engines are scrolling and searches are based on interconnected servers. Interconnected servers mean that you interact regularly with the source, but this does not happen when it comes to the dark web. All is behind the veil and is hidden internally in the Tor network, guaranteeing security and privacy. Only 4% of Internet content is accessible to the general public and the remaining 96% is hidden behind the deep web.

Now, the reason that Google does not collect these data or why profound web content is not indexed is not a secret. These companies are primarily illegal or bad for society as a whole. The content can be porn, drugs, arms, military information, hacking tools and so on. Robots Exclusion The robot.txt we normally use is to tell the website which of the files it is supposed to record and register. Now we have a terminology called "exclusion files for robots."

Web administrators will tweak the setup so that certain pages do not appear for indexing and remain hidden when searching for the scanners. Let's look at some of the screwdrivers in the internet.

Some of the more reasons why Traditional Search Engines do not index these type of Deep Web Search content are described below, hence we have described some of the properties of the Deep Web Search Engines. These Deep Web resources may contain complex databases which are not easily understood by the Search Engine bots and thus not indexed also. Such Non-Indexed Content may include Contextual Web, Dynamic Content, Limited Access Content, Non-HTML Content, Private Web Content, Software, Archives etc. Coming a little out from the world of Deep Web Search Engine, and reviewing the Deep Web Search. There is no any such thing that a Deep Web Search Engine is necessary to browse the Deep Web but it the only Best option to browse the Deep Web. We can also browse the Deep Web using a lot of other ways or methods. In other words, we may say that Deep Web Search Engines are one of the Best options to choose to search the Web Deeply.

Top Deep Web Search Engines

- **Torch** - Torch has one of the largest search engines in the deep web, as they claim to have an index of more than a million hidden page results. It is one of the oldest search engines. Same as notEvil this search engine also having very easy layout, only having one text box for searching one button. Here you only need put your query on search engine box and hit search button, holla result on front of your eyes. Torch is working just like as Google search engine, when you searched any query that you will got good no or result.
- **DuckDuckGo** - This deep web search engine—which, like many other deep web search engines on this list, also lets you search the regular web—has a clean and easy to use interface and doesn't track your discoveries. The options for topics to search are endless, and you can even customize it to enhance your experience.
- **Onion URL Repository** - The Onion URL Repository has a massive index of over a million page results and does not set limits on what information it holds close.
- **Uncensored Hidden Wiki** - When you search the deep web occasionally, you'll discover useful places where you need to be careful. The Uncensored Hidden Wiki is very much one of those locations, an uncensored collection of links and articles that, over the site's history, have included links to information on criminal activities from drugs to child pornography. The site has cleaned up its act considerably, but there are still links to graphic content and possibly illegal sites to be found. If you can look past those elements, however, Uncensored Hidden Wiki is a treasure trove of deep web information. Inside you'll discover blogs about Tor, links to deep web email services, and even social networks. Just be careful what you search.
- **notEvil** - This search engine is great because users can skip all the clutter and distraction from surfing the web with no ads. It's clean and mimics the look of Google. The search engines not for profit' not Evil' completely survive on contribution and it seems to receive a fair share of support. Highly reliable in search results, this SE has a highly competitive functionality in the TOR network. This search engine provides all type search result by the help of Query or URL, means if you having query and want to find result related to your query then notEvil can help you. notEvil also can search by the help url, and can find your result very quick. One more thing when you will search any query on this search engine, and you not found any good result, then this search engine chat service can help you.

- **ParaZite** - The deep web can seem like a terrifying place, but part of the fun of discovery is opening doors and not knowing what's behind them. ParaZite is a search engine that gamified the deep web. Beyond its basic, and useful, search features, it also offers up the chance to gamble by taking you to a random site on the deep web. It's basically the deep equivalent of Google's "Feeling Lucky" feature—except using it I was taken to a new email client, a black market site, and an essay on why children are jerks. Make sure you're using a firewall and VPN before you fire up ParaZite.
- **TorLinks** - The directory in TorLinks has a wide range of intellectual results, with the most notable being the literary section.
- **Grams** - This is the search engine to end all drug-related hunts. Down in the depths, users are able to search effectively for the dark net drugs that are available for purchase on the majority of web page results.
- **Touchgraph** - Touchgraph gets visual with the deep web scavenger hunt. The algorithm it uses is specifically designed to cluster the relationship between your search results to create a visual result—a creative touch to make searching more exciting.
- **Ahmia.fi** - Ahmia.fi is a great search engine for beginners who are new to the deep web. It takes about five seconds to figure out how the search engine works. Once cracked, scouring the deep web becomes a breeze. Ahmia is another top deep web search engine, which deep web user's likes to find his required results, I also used Ahmia many time for search. Same as other deep web search engine, Ahmia also offering query searching service, means put your query into search text box and press search button and get result. It offers some great services like Ahmia viewer, add .onion links into Ahmia database, I2P Seraching. Ahmia automatically detect bad .onion links and blacklisted into his database, and also maintain his most link visit charts which you can see by the help of <http://msydstlz2kzerdg.onion/stats/viewer> links.
- **Yippy** - Like Touchgraph, this search engine also collects your searches to make a common result or pattern, but without the visual aspect. Instead, it's simple like Google. It is a Meta search engine (it gets its results by using other web indexes), I've included Yippy here because it has a place with a device entry for a web client, e.g. email, games, videos and so on.
- **Candle Search Engine** - Candle is another alternative for deep web search engine; this is also popular into deep web community, everyday people use this search engine, I also try this search engine many time for deep web searching. Candle search engine does not allow parentheses, Boolean operators; any type quotes into search query, if you put any of these types' things into search query, then you wouldn't get required results. Only you can try simple words, For Example, Today I am searching query "deep web links" then I put my query into search box then hit enter, now I am getting some results on my computer screen, but result have only those type sites which have .onion extension domain.
- **Searx Search Engine** - Searx is another alternative search engine for deep web, this search engine also working on free information, if you search here anything then Searx not maintain your log file. This is simple means no one can trace your all activity which you will perform on Searx search engine, here you can search anything which you want. One thing is very good in Searx, This search engine is open source search engine, you can modify Searx source code according to you and also you can participate in search engine functions enhance program. Searx search engine is a great program which collects data from multiple popular search engine like Google, Bing and Yahoo. But here I saw one common thing if any website have high ranking into multiple search engine then searx give top position into search result. Searx search engine is not able to search .onion

domain sites. If you try to search anything about .onion sites related then you cannot get required result. Searx search engine offer one great feature which is file related search, you can select any file related option which type results you want to get.

- **Archive.org** - Maybe this was the very first Deep Web Search Engine, I ever found. And also is the top of the most useful websites ever available on the Internet. According to them, they are the non-profit library of millions of this like books, movies, software, music etc. As mentioned on their homepage, they have about 466 billion web pages saved in their database. They have the screenshot of almost every website ever visited on the Internet. You can just image how big this database. Owing to its bigness, how precious and valuable it is. On this search engine, you can know how different websites, which are now touching the heights of the Internet were actually looks like when they were in the starting days. You can see how Google looks when it was started. You can see how Bing looks when it was started. Similarly, you can see almost each and every site's history webpages. This feature of this ultimate search engine is popularly known as the WayBackMachine, which may took you to the olden times of the Internet.
- **Vlib.org** - This is also a Deep Web Search Engine with a very much vast Database. You can browse through a lot of categories which includes Agriculture, Information and Libraries, Computing and Computer Science, Regional Studies and much more. This is also one of the oldest deep web search engine on the Internet.
- **Wolfram Alpha: Computational Knowledge Engine** - This Deep Web Search Engine one of the Best ever website I have ever found on the Internet which impressed me in the first visit. As mentioned, it is computational knowledge search engine which will show you the results based on the things related to calculation and computational things. On the official homepage, there have given a lot of things that we can do with Wolfram Alpha. Some of them are mentioned below. Mathematics, Step by Step Solutions, Statistical & Data Analysis, History, Media, Finance, Physics, Engineering, Geography, Chemistry, Education, Web and Computers and much more. Here is an example search made in the Mathematics section of the Wolfram Alpha Deep Web Search Engine. Mathematics, Step by Step Solutions, Statistical & Data Analysis, History, Media, Finance, Physics, Engineering, Geography, Chemistry, Education, Web and Computers and much more. Here is an example search made in the Mathematics section of the Wolfram Alpha Deep Web Search Engine.
- **Deep Web Tech (DeepWebTech.com)** - This is one another example of the Deep Web Search Engine. In this deep web search engine, you may browse multiple other deep web search engines such as the science.gov. Science.gov is also one of the most popular deep web search engine where you can find the information and resources related to US federal science.
- **Kilos** - Kilos is a dark web search engine by all definitions. It was created with the sole purpose of letting users search for "Drugs" on the dark web. It fetches results from all the indexed Darknet markets on the Dark web (currently 6) as well as from forums. Even displays "featured listings" on the left-sidebar.

How Dark Web Search Engine Works and their way of Indexing

Search engines like Google are incredibly powerful, but they can't crawl and index the vast amount of data that is not hyperlinked or accessed via public DNS services. However, there are Deep Web Search Engines that crawl over the TOR network and bring the same result to your regular browser. These Deep Web search engines talks to the onion service via Tor and relays, resolve the .onion links and

then deliver the final output to your regular browser on the ordinary World Wide Web. We all know websites of Deep & Dark Web are not indexed, then how Dark Web Search Engines work?

According to Google's online dictionary, the deep web is "the part of the World Wide Web that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks". It is estimated that search engines like Google index only 4% of the entire world wide web, meaning that the deep web is nearly 25 times larger than the internet you and I have used our whole lives. Note: the deep web shouldn't be confused with the "dark web", which pertains strictly to pages containing illegal content such as child pornography, terrorist forums, and illegal auctions/transactions.

Google's search engine functions by using "crawlers". These crawlers start from a list of known web addresses, visit those pages, then follow the links contained on those pages, and continue following links found on the new pages, collecting information about each page as they go. Now, consider a single page in the deep web. Google's search engine could be unable to find this page because of several reasons. For one, Google's crawlers might never come across this page simply because no other previously crawled page links to it. Additionally, this page might require some sort of authentication such as filling out a search form and clicking submit, or having a certain certificate. Also, if a page contains illegal content, Google will likely not want that content appearing in search results, so they won't index it. Finally, if the creator of a page doesn't want it to be indexed by popular search engines, they can include a suitable robots.txt file, which tells the crawlers not to index the page. If the crawlers index the page anyways, then legal action can be taken against the creator of the crawlers, and the search engine can end up on a bot reporting site like <http://www.botreports.com/badbots/>.

Now for example, we consider Ahmia – a deep web search engine to understand how it searches the deep web or dark web. Ahmia essentially collects .onion URLs from the Tor network, then feeds these pages to their index provided that they don't contain a robots.txt file saying not to index them. Additionally, Ahmia allows onion service operators to register their own URLs, enabling them to be found. Through continuously collecting .onion URLs, Ahmia has created one of the largest indexes of the deep web. But it is true that it still comes nowhere near to scratching the surface of the whole deep web, but it indexes a good portion of the content that most people would want to look for.

We can use another example such as Uncensored Hidden Wiki. It operates differently. Anyone can register on the Uncensored Hidden Wiki, and after that, anyone can edit the links contained in the database. The search engine operates by searching the provided descriptions of the pages at these links. This certainly has its pros and cons. On the bright side, crowd-sourcing the links is one of the best ways to collect a large number of useful URLs, and keep them up to date (especially since .onion domain names change extremely often). On the other hand, anyone can change the links to wherever they want, or alter the descriptions of the links. The negatives of this can be mitigated by site admins to ensure that the links are usually accurate, but there are no guarantees when using the links on this page. Additionally, the Uncensored Hidden Wiki has its name for a reason, as the content of that page is certainly uncensored.

While the "deep web search engines" mentioned above are capable of indexing a good part of the deep web, the vast majority of it remains unindexed, and no search engine is capable of finding everything contained in it. The best deep web search engines function in various ways, whether it be

crowd-sourcing URLs and page descriptions or continuously collecting them, but they certainly do not function in similar ways to traditional search engines such as Google. If you want to learn more about the deep web, you can find plenty of information about the deep web using Google (how ironic). If you want to search the deep web yourself, here's my advice: don't. Especially if you've never heard of terms like .onion, Tor gateways, proxies, botnets, Trojans, etc. If you're anything like me then you have no business searching the deep web, as it can be dangerous if you're not extremely careful protecting your identity, even when using the search engines mentioned above in conjunction with the Tor browser. The deep web also has very little that you or I would find interesting, and plenty of things that neither you nor I want to see.

Surface Web Search Engine

Search engines are answer machines. They scour billions of pieces of content and evaluate thousands of factors to determine which content is most likely to answer your query.

A search engine is software, usually accessed on the Internet that searches a database of information according to the user's query. The engine provides a list of results that best match what the user is trying to find. Today, there are many different search engines available on the Internet, each with their own abilities and features. The first search engine ever developed is considered Archie, which was used to search for FTP files and the first text-based search engine is considered Veronica. Currently, the most popular and well-known search engine is Google. Other popular search engines include AOL, Ask.com, Baidu, Bing, and Yahoo.

How a search engine works

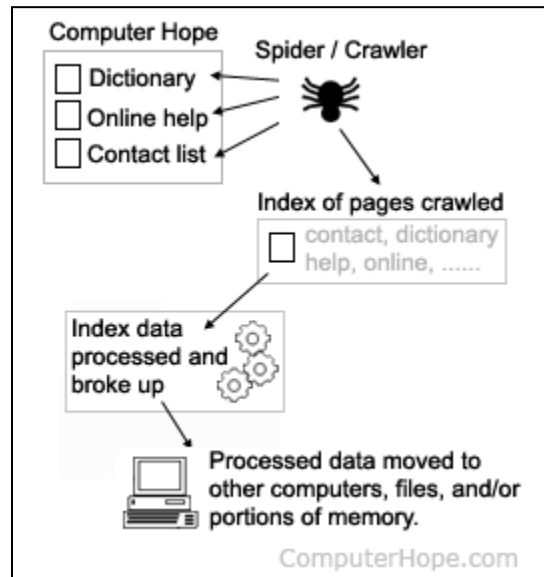
Because large search engines contain millions and sometimes billions of pages, many search engines not only search the pages but also display the results depending on their importance. This importance is commonly determined by using various algorithms.

As illustrated in the image on the right, the source of all search engine data is a spider or crawler, which automatically visits pages and indexes their contents.

Once a page is crawled, the data contained in the page is processed and indexed. Often, this can involve the steps below.

- Strip out stop words.
- Record the remaining words in the page and the frequency they occur.
- Record links to other pages.
- Record information about any images, audio, and embedded media on the page.

The data collected is used to rank each page. These rankings then determine which pages to show in the search results and in what order. Finally, once the



data is processed, it is broken up into one or more files, moved to different computers, or loaded into memory where it can be accessed when a search is performed.

Search engines use proprietary algorithms to index and correlate data, so every search engine has its own approach to finding what you're trying to find. Its results may be based on where you're located, what else you've searched for, and what results were preferred by other users searching for the same thing, for example. Each search engines will weigh these factors in a unique way, and offer you different results.

Search engines have three primary functions:

1. **Crawl:** Scour the Internet for content, looking over the code/content for each URL they find.
2. **Index:** Store and organize the content found during the crawling process. Once a page is in the index, it's in the running to be displayed as a result to relevant queries.
3. **Rank:** Provide the pieces of content that will best answer a searcher's query, which means that results are ordered by most relevant to least relevant.

Crawling - Crawling is the process by which search engines discover updated content on the web, such as new sites or pages, changes to existing sites, and dead links.

To do this, a search engine uses a program that can be referred to as a 'crawler', 'bot' or 'spider' (each search engine has its own type) which follows an algorithmic process to determine which sites to crawl and how often.

As a search engine's crawler moves through your site it will also detect and record any links it finds on these pages and add them to a list that will be crawled later. This is how new content is discovered.

Indexing - Once a search engine processes each of the pages it crawls, it compiles a massive index of all the words it sees and their location on each page. It is essentially a database of billions of web pages.

This extracted content is then stored, with the information then organized and interpreted by the search engine's algorithm to measure its importance compared to similar pages.

Servers based all around the world allow users to access these pages almost instantaneously. Storing and sorting this information requires significant space and both Microsoft and Google have over a million servers each.

Indexing is the process by which search engines organize information before a search to enable super-fast responses to queries. Searching through individual pages for keywords and topics would be a very slow process for search engines to identify relevant information. Instead, search engines (including Google) use an inverted index, also known as a reverse index.

Reverse Index - An inverted index is a system wherein a database of text elements is compiled along with pointers to the documents which contain those elements. Then, search engines use a process called tokenization to reduce words to their core meaning, thus reducing the amount of resources needed to store and retrieve data. This is a much faster approach than listing all known documents against all relevant keywords and characters.

Cached version of A Page - In addition to indexing pages, search engines may also store a highly compressed text-only version of a document including all HTML and metadata.

The cached document is the latest snapshot of the page that the search engine has seen.

The cached version of a page can be accessed (in Google) by clicking the little green arrow next to each search result's URL and selecting the cached option. Alternatively, you can use the 'cache:' Google search operator to view the cached version of the page.

Bing offers the same facility to view the cached version of a page via a green down arrow next to each search result but doesn't currently support the 'cache:' search operator.

PageRank - "PageRank" is a Google algorithm named after the co-founder of Google, Larry Page (yes, really!) It is a value for each page calculated by counting the number of links pointing at a page in order to determine the page's value relative to every other page on the internet. The value passed by each individual link is based on the number and value of links which point to the page with the link.

PageRank is just one of the many signals used within the large Google ranking algorithm. An approximation of the PageRank values were initially provided by Google but they are no longer publicly visible.

While PageRank is a Google term, all commercial search engines calculate and use an equivalent link equity metric. Some SEO tools try to give an estimation of PageRank using their own logic and calculations. For example, Page Authority in Moz tools, TrustFlow in Majestic, or URL Rating in Ahrefs. DeepCrawl has a metric called DeepRank to measure the value of pages based on the internal links within a website.

How PageRank flows through pages

Pages pass PageRank, or link equity, through to other pages via links. When a page links to content elsewhere it is seen as a vote of confidence and trust, in that the content being linked to is being recommended as relevant and useful for users. The count of these links and the measure of how authoritative the linking website is, determines the relative PageRank of the linked-to page.

PageRank is equally divided across all discovered links on the page. For example, if your page has five links, each link would pass 20% of the page's PageRank through each link to the target pages. Links which use the rel="nofollow" attribute do not pass PageRank.

How Search Engine Indexing Works (In Detail)

Once the spiders have completed the task of finding information on Web pages (and we should note that this is a task that is never actually completed -- the constantly changing nature of the Web means that the spiders are always crawling), the search engine must store the information in a way that makes it useful. There are two key components involved in making the gathered data accessible to users:

- The information stored with the data
- The method by which the information is indexed

In the simplest case, a search engine could just store the word and the URL where it was found. In reality, this would make for an engine of limited use, since there would be no way of telling whether the word was used in an important or a trivial way on the page, whether the word was used once or many times or whether the page contained links to other pages containing the word. In other words, there would be no way of building the ranking list that tries to present the most useful pages at the top of the list of search results.

To make for more useful results, most search engines store more than just the word and URL. An engine might store the number of times that the word appears on a page. The engine might assign a weight to each entry, with increasing values assigned to words as they appear near the top of the document, in sub-headings, in links, in the Meta tags or in the title of the page. Each commercial search engine has a different formula for assigning weight to the words in its index. This is one of the reasons that a search for the same word on different search engines will produce different lists, with the pages presented in different orders.

Regardless of the precise combination of additional pieces of information stored by a search engine, the data will be encoded to save storage space. For example, the original Google paper describes using 2 bytes, of 8 bits each, to store information on weighting -- whether the word was capitalized, its font size, position, and other information to help in ranking the hit. Each factor might take up 2 or 3 bits within the 2-byte grouping (8 bits = 1 byte). As a result, a great deal of information can be stored in a very compact form. After the information is compacted, it's ready for indexing.

An index has a single purpose: It allows information to be found as quickly as possible. There are quite a few ways for an index to be built, but one of the most effective ways is to build a hash table. In hashing, a formula is applied to attach a numerical value to each word. The formula is designed to evenly distribute the entries across a predetermined number of divisions. This numerical distribution is different from the distribution of words across the alphabet, and that is the key to a hash table's effectiveness.

In English, there are some letters that begin many words, while others begin fewer. You'll find, for example, that the "M" section of the dictionary is much thicker than the "X" section. This inequity means that finding a word beginning with a very "popular" letter could take much longer than finding a word that begins with a less popular one. Hashing evens out the difference, and reduces the average time it takes to find an entry. It also separates the index from the actual entry. The hash table contains the hashed number along with a pointer to the actual data, which can be sorted in whichever way allows it to be stored most efficiently. The combination of efficient indexing and effective storage makes it possible to get results quickly, even when the user creates a complicated search.

Indexing: How do search engines interpret and store your pages?

Once you've ensured your site has been crawled, the next order of business is to make sure it can be indexed. That's right — just because your site can be discovered and crawled by a search engine doesn't necessarily mean that it will be stored in their index. In the previous section on crawling, we discussed how search engines discover your web pages. The index is where your discovered pages are stored. After a crawler finds a page, the search engine renders it just like a browser would. In the process of doing so, the search engine analyzes that page's contents. All of that information is stored in its index.

Are pages ever removed from the index?

Yes, pages can be removed from the index! Some of the main reasons why a URL might be removed include:

- The URL is returning a "not found" error (4XX) or server error (5XX) – This could be accidental (the page was moved and a 301 redirect was not set up) or intentional (the page was deleted and 404ed in order to get it removed from the index)

- The URL had a noindex Meta tag added – This tag can be added by site owners to instruct the search engine to omit the page from its index.
- The URL has been manually penalized for violating the search engine's Webmaster Guidelines and, as a result, was removed from the index.
- The URL has been blocked from crawling with the addition of a password required before visitors can access the page.

If you believe that a page on your website that was previously in Google's index is no longer showing up, you can use the URL Inspection tool to learn the status of the page, or use Fetch as Google which has a "Request Indexing" feature to submit individual URLs to the index. (Bonus: GSC's "fetch" tool also has a "render" option that allows you to see if there are any issues with how Google is interpreting your page).

Search Engine Ranking Process

When someone performs a search, search engines scour their index for highly relevant content and then orders that content in the hopes of solving the searcher's query. This ordering of search results by relevance is known as ranking. In general, you can assume that the higher a website is ranked, the more relevant the search engine believes that site is to the query.

It's possible to block search engine crawlers from part or all of your site, or instruct search engines to avoid storing certain pages in their index. While there can be reasons for doing this, if you want your content found by searchers, you have to first make sure it's accessible to crawlers and is indexable. Otherwise, it's as good as invisible.

4 Experiments

There are no broad discussions or procedures can be found on the internet on scraping the Dark Web. Our research purpose was to explore the E-commerce world of Dark Web and try to scrape or crawl the websites so that we could analyze the structures of e-commerce websites on dark web. By structure we mean that the html structure of the website, the content type and format that dark web developers prefer to include on the websites etc.

But due to the unavailability of a proper dark web scraper, we couldn't be able to crack how to do it successfully. The first question is, can dark websites be scraped or crawled? The answer is, yes. Dark Web can be scraped and crawled. The problem is the availability of the scraper.

Our Attempts

We found some dark web scraper on GitHub. For example there is a developer who developed OSINT tool for scraping dark websites. The code is written in Python. We tried that code but doesn't work. Maybe because the developer tried it in Kali Linux and also the instructions are not so clear, or maybe the lack of our skill which results in failure. However we found 2-3 other scraper in GitHub which also doesn't work. There are websites like X-Byte enterprise crawling and iWeb scraping who offers good scraping tools but they all are paid tools.

We faced more challenges like security issues as we were trying to test the available tools from our personal pc, scraping is something that can create a high chance of exposing our IP address to the hackers

around the dark web. So we couldn't just attempt some riskier task which may provide us the success but also expose our IP address on the dark web. There was also no one who will guide us to the proper path we should in the way of crawling dark web.

Some Information and Descriptions about tools that we failed to use:

TorBot is an open source intelligent tool that can be helpful for us for scraping dark web. It can be found on GitHub where 24 contributors are working on this. It includes .onion crawler as well. But the basic setup was complex, we failed to do the basic setup before installing it. But the features and description of it are written below just to inform about it.

If you're looking for an advanced tool for dark web research, TorBot probably is and will continue to be overkill. As of this writing, the last update to TorBot was in February. It uses Python 3.x and requires a Tor dependency. TorBot has a list of features that makes it useful for multiple applications. Features include:

1. Onion Crawler (.onion).
2. Returns Page title and address with a short description about the site.
3. Save links to database.
4. Get emails from site.
5. Save crawl info to JSON file.
6. Crawl custom domains.
7. Check if the link is live.
8. Built-in Updater.

OS Dependencies -

- Tor
- Python 3.x

Python Dependencies –

- BeautifulSoup4
- Pyinstaller
- PySocks
- Termcolor
- Requests
- requests_mock
- yattag

Fresh Onions

Fresh Onions is a tool that hasn't been updated in a while. As a disclaimer, you may have issues running the script as 2017 was the last GitHub push. However, even as an academic piece of what is possible on the dark web using Python, it's worth taking a look at what features this tool offers or once offered. Here's a list of the features:

- Crawls the darknet looking for new hidden service
- Find hidden services from a number of clearnet sources
- Optional fulltext elasticsearch support
- Marks clone sites of the /r/darknet superlist
- Finds SSH fingerprints across hidden services
- Finds email addresses across hidden services
- Finds bitcoin addresses across hidden services
- Shows incoming / outgoing links to onion domains
- Up-to-date alive / dead hidden service status
- Portscanner
- Search for "interesting" URL paths, useful 404 detection
- Automatic language detection
- Fuzzy clone detection (requires elasticsearch, more advanced than superlist clone detection)

Infrastructure of Fresh Onions

Fresh Onions runs on two servers, a frontend host running the database and hidden service web site, and a backend host running the crawler. Probably most interesting to the reader is the setup for the backend. TOR as a client is COMPLETELY SINGLETHREADED. I know! It's 2017, and along with a complete lack of flying cars, TOR runs in a single thread. What this means is that if you try to run a crawler on a single TOR instance you will quickly find you are maxing out your CPU at 100%.

The solution to this problem is running multiple TOR instances and connecting to them through some kind of frontend that will round-robin your requests. The Fresh Onions crawler runs eight Tor instances.

Debian (and ubuntu) comes with a useful program "tor-instance-create" for quickly creating multiple instances of TOR. I used Squid as my frontend proxy, but unfortunately it can't connect to SOCKS directly, so I used "privoxy" as an intermediate proxy. You will need one privoxy instance for every TOR instance. There is a script in "scripts/create_privoxy.sh" to help with creating privoxy instances on debian systems. It also helps to replace /etc/privoxy/default.filter with an empty file, to reduce CPU load by removing unnecessary regexes.

TorCrawl

Another crawling tool developed in Python. TorCrawl not only crawls hidden services on Tor, it extracts the code on the services' webpage. So, what is this useful for? In a world with infinite time, you could setup and run TorBot, figure out how to get everything running, and have a reliable tool that will consistently get new DLCs. In a semi perfect world you'd have the time to database services with subscriptions, manual tools, and Fresh Onions, then inspect each onion webpage for possible malicious content, then manually inspect each page for your investigation. But it's not a perfect world and in most cases, the Pareto Principle applies and you have to get the most amount of work done in the least amount of time. So instead of worrying about crawling, inspection, then investigation, do it all in one with TorBot. You get the webpage markup so you can view the content without having to physically access the page. You can also view the static webpage by saving it as an .html file.

5 Acknowledgments

This Project Research work is the under part of our academic course CSE499 A & B as titled "Senior Design Project". We guided this research work under the supervision of Mohammad Ashrafuzzaman Khan sir. And we are very grateful to him for giving us a great opportunity to work on such interesting topic. Therefore, the full procession of this research work, we got to learn and know many interesting thing about deep dark web which is vast knowledge of internet and we are eagerly waiting to publish a paper about this topic under our supervisor.

5 References

- Barbosa, L. and Freire, J. (2004). Siphoning Hidden-Web Data through Keyword-Based Interfaces. In Proceedings of the SBBD.
- Bergman, M. K. (2000). The Deep Web: Surfacing Hidden Value. BrightPlanet.com,
- Burris, V., Smith, E., and Strahm, A. (2000). White Supremacist Networks on the Internet. Sociological Focus, 33(2), 215-235.
- Chakrabarti, S., Van Den Berg, M., and Dom, B. (1999). Focused Crawling: A New Approach to Topic-Specific Resource Discovery. In Proceedings of the Eight World Wide Web Conference, Toronto, Canada.
- Crilley, K. (2001). Information Warfare: New Battle Fields Terrorists, Propaganda, and the

Internet. In Proceedings of the Association for Information Management, 53(7), 250-264.

Gareth Owen. N. S. (2015). The Tor Dark Net, 30

September 2015. [Online]. Available: [https://](https://www.cigionline.org/publications/tor-dark-net)

www.cigionline.org/publications/tor-dark-net.

Hawkins, B. (2016). Under The Ocean of the Internet

- The Deep Web, 15 May 2016. [Online]. Available: [https:/](https://www.sans.org/reading-room/whitepapers/covert/oceaninternet-deep-web-37012)

[/www.sans.org/reading-room/whitepapers/covert/oceaninternet-deep-web-37012](https://www.sans.org/reading-room/whitepapers/covert/oceaninternet-deep-web-37012).

Finklea, K. Dark Web, 10 March 2017. [Online].

Available: <https://fas.org/sgp/crs/misc/R44101.pdf>.

Ling Liu, M. T. O. z. (2018). Encyclopedia of database

systems, Springer.

<https://www.technadu.com/best-dark-web-sites/68920/>

<https://www.technadu.com/dark-web-history/52017/>

<https://hackwarenews.com/the-dark-web-a-history-lesson/>

<https://www.truthfinder.com/dark-web/>

<https://protonirockerxow.onion>

<https://www.whoishostingthis.com/blog/2017/07/27/ecommerce-problems/>

<https://www.geeksforgeeks.org/dark-web-analytics-and-interesting-facts-behind-its-anonymity/>

<https://www.thebalancesmb.com/advantages-of-ecommerce-1141610>

<https://www.elliptic.co/>

Bayati, S., Bahreininejad, A., Nejad, A. and Kharazmi, S. (2010). Improving Semantic Web Services Composition Performance, Using Data Mining Techniques. *Journal of Algorithms & Computational Technology*, 4(4), pp.409-423.

Berendt, B., Hotho, A. and Stumme, G. (2010). Bridging the Gap—Data Mining and Social Network Analysis for Integrating Semantic Web and Web 2.0. *Web Semantics: Science, Services and Agents on the World Wide Web*, 8(2-3), pp.95-96.

Bradbury, D. (2014). Unveiling the dark web. *Network Security*, 2014(4), pp.14-17.

Chen, H. (2012). *Dark web*. New York, NY: Springer.