**E-Commerce World of Dark Web**



Anwar Shadaab 1611383042

Rahat Rakib

Sumaya

Raihan

Date

CSE499B: Senior Project

Mohammad Ashrafuzzaman Khan

**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**

**List of Figures**

**List of Tables**

**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 implement their business strategies 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.

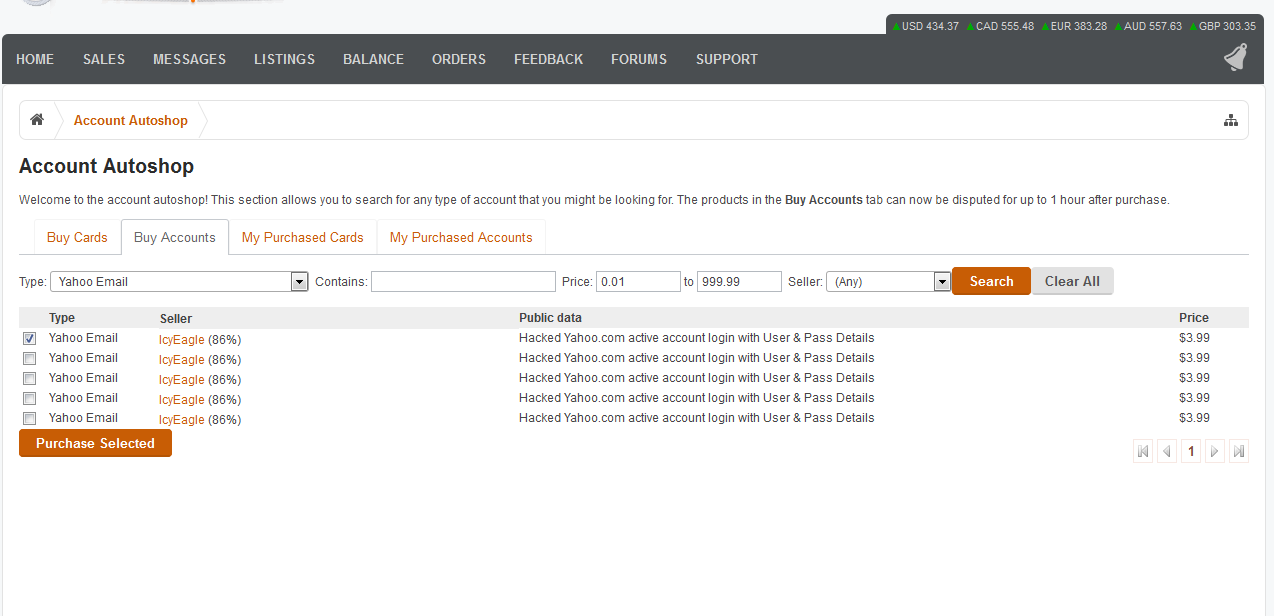
5. **Poor Content and Product Descriptions:** Many e-commerce stores Product descriptions came into sharp focus since many stores were using thin or generic text. Customers read the content and description before buying it online.

**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?

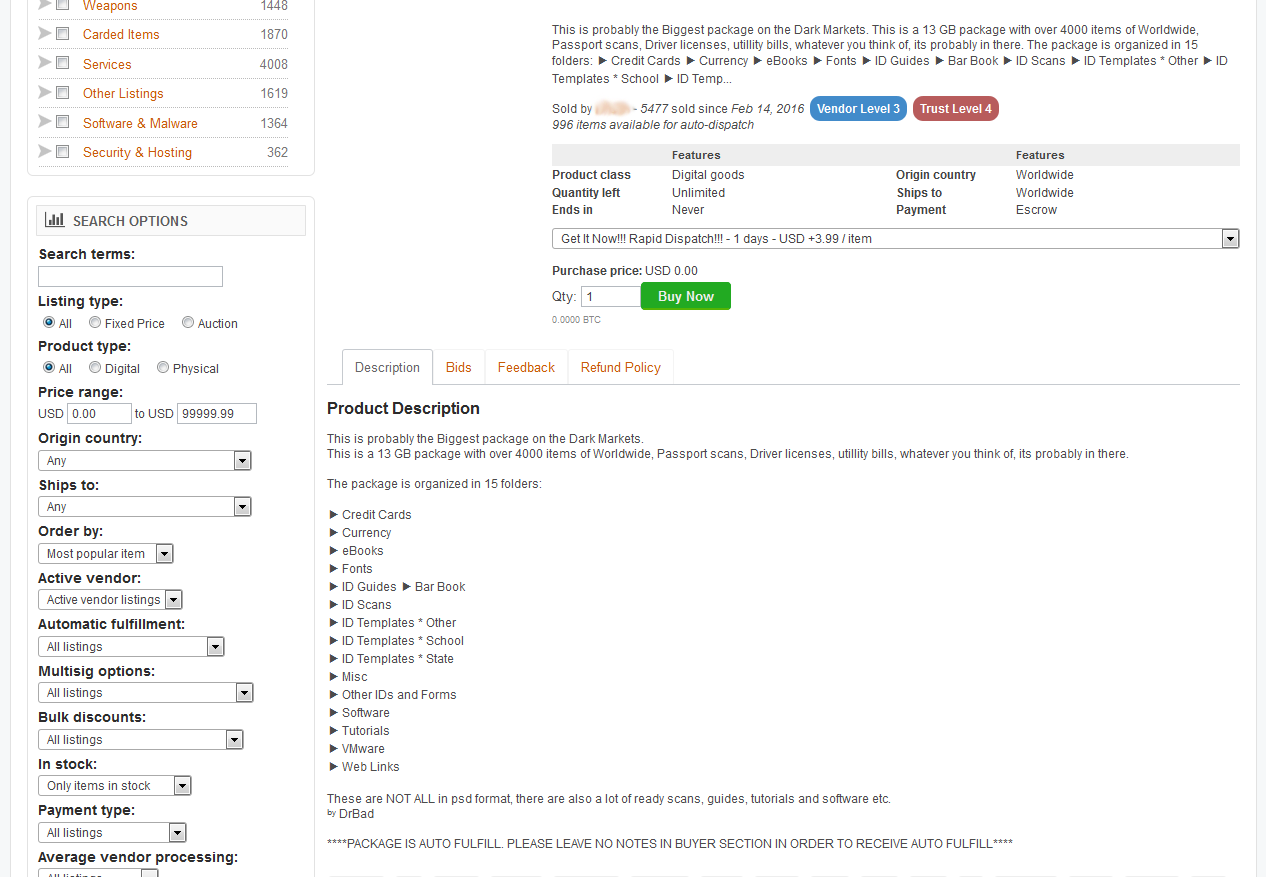
Dark web commerce sites have the same features as any e-retail operation, including ratings/reviews, shopping carts and forums, but there are important differences. One is quality control. When both buyers and sellers are anonymous, the credibility of any ratings system is dubious. Ratings are easily 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 “autoshop” 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**

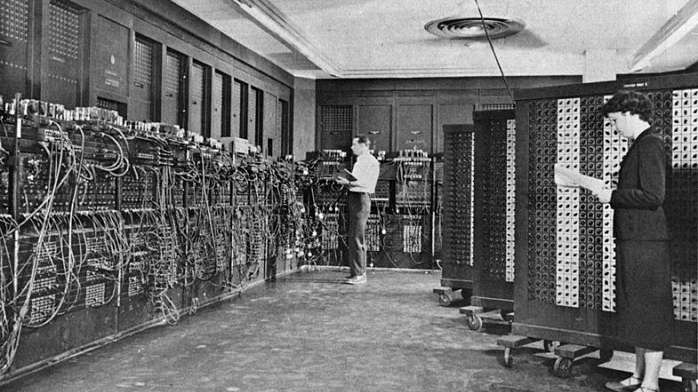
Buyers and sellers of niche products can find it difficult to locate each other in the physical world. Online, it is only a matter of the customer searching for the product in a search engine. One example could be the purchase of obsolete parts. Instead of trashing older equipment for lack of spares, 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 lead to a massive shakeup of the music industry. Thanks to like 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 alike 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 as 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. Ironic, 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.

[](https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/)

***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.

[](https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/)

***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 found 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%

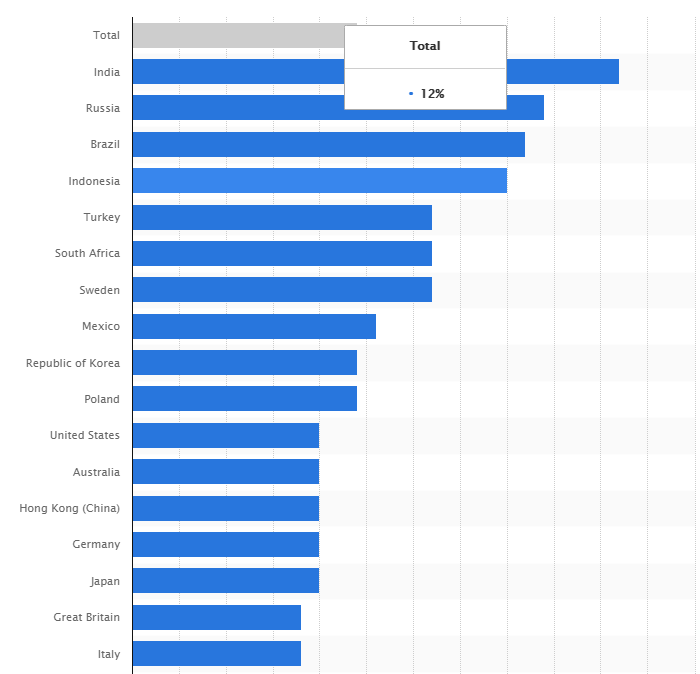
• Sweden 16%

• Mexico 13%

• Korea 12%

• Poland 12%

And so on.



***Fig 11: Percentage of User access into Dark Web***

**Some Statistics & Facts**

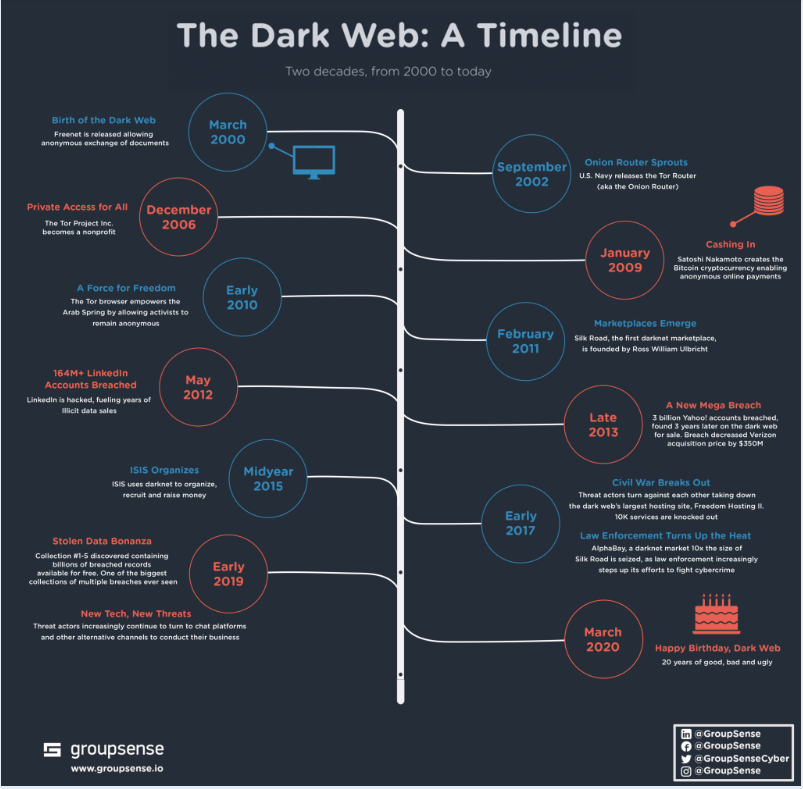
**At least 100 darknet marketplaces were active 2019:** Darknet marketplaces are where one can find everything ranging from marijuana to rocket launchers. There would be sellers offering credit card info and email IDs too. Human trafficking is often associated with these marketplaces, as well. Authorities 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

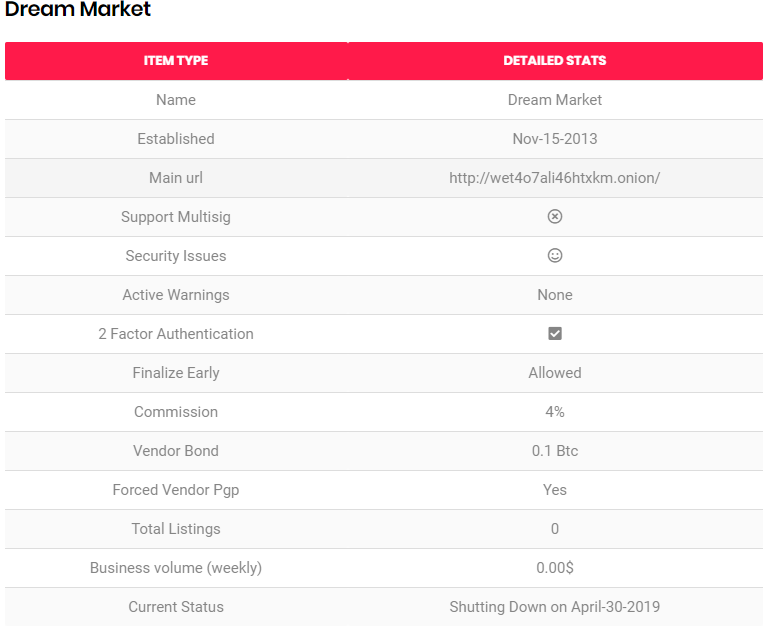
• No communication with the outside world

• $255k is the total payment for 6 months

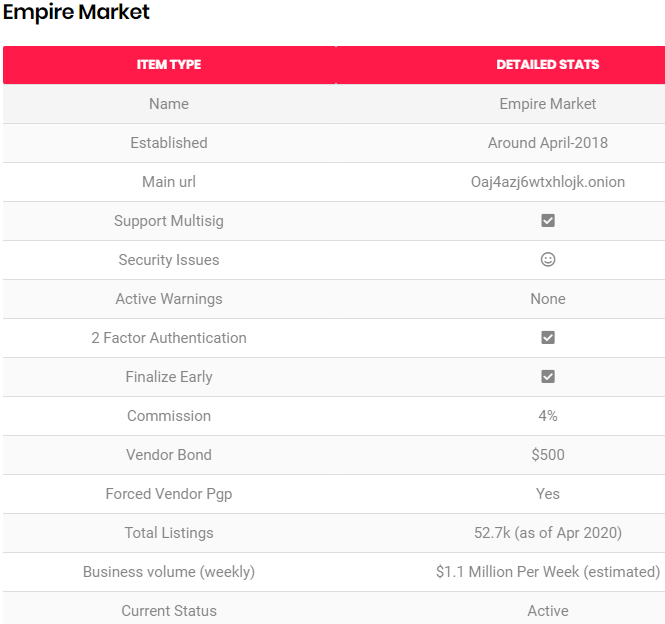
**Five Guys:** According to a Reddit post, "Was on Tor, browsing da usuals. Go out to eat foods at the Five Guys. Come back. More Tor. Find a picture of me eating at Five Guys.”

**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**

****

***Fig 13: Dream Market***

****

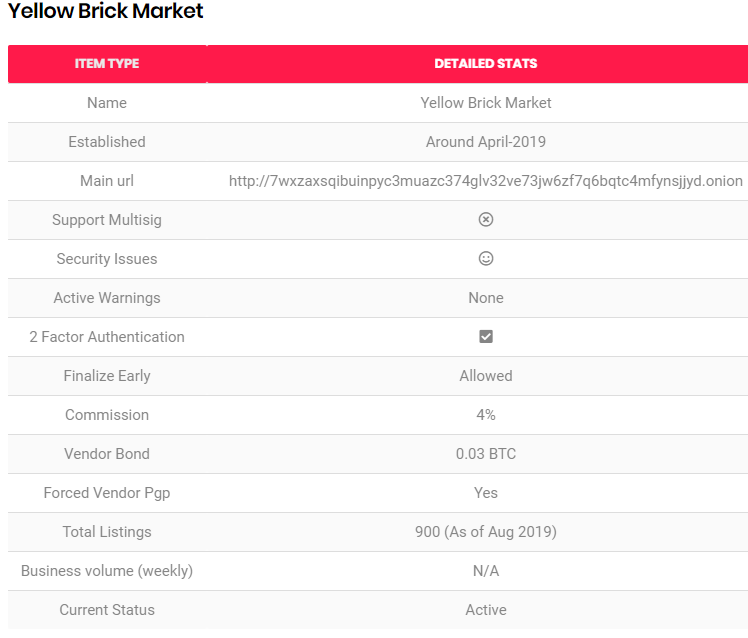
***Fig 14: Empire Market***

****

***Fig 15: Big Blue Market***

****

***Fig 16: Agartha Market***

****

***Fig 17: Yellow Brick Market***

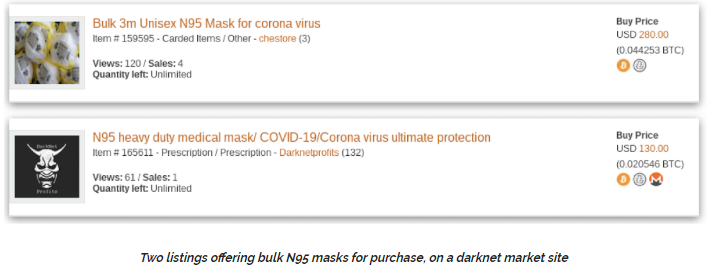
**3.5 How Dark Web Markets Are Exploiting the Coronavirus Pandemic**

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.



***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.

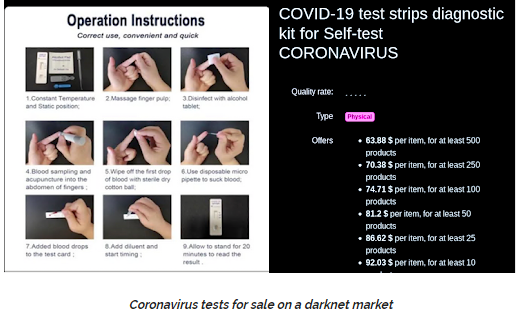
Beyond the usual dark marketplaces, a new online shop has launched - dedicated to the sale of masks. The operator of this site claims to be a European wholesaler for hospitals, but believes that “Everybody need a chance to get a Mask for protection - Not only medical employees!”



***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.



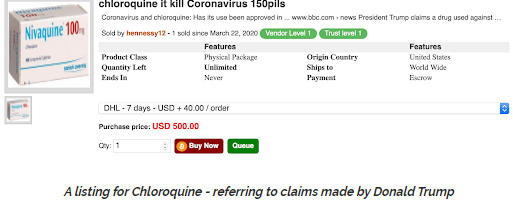
***Fig 20: Coronavirus tests for sale***

**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.



***Fig 21: A listing for Chloroquine***



***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***

**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**

**6 References**

**Appendix A:**