An Evaluation of the Secure End User Experience on the Darknet

Nathaniel Milliken
University of Denver

1 ABSTRACT

The world wide web is a vast interconnected network of hypertext links. The darknet, which accounts for less than one half of a percent of the web is a community dedicated to the anonymity of users. The darknet has many use cases for the end user. There are countless reasons to want to maintain anonymity, for example journalism in an authoritarian regime, or learning to hack through blackhat forums, or buying drugs from vendors all across the world. This paper focuses on the experience of the end user on the darknet. Through our systematic review of the small but ever expanding database of articles relating to users on the darknet, we build a comprehensive discussion about anonymity, and the potential revocation of that anonymity. In this paper, the emphasis is on continuing to allow the darknet user to remain anonymous.

2 INTRODUCTION

In this systematic review, we focused on research papers of high quality that related to our topic of end user experience on the darknet. Of the relevant articles, only one was actually found to be a user study [measuring effects of technical mechanisms on reported user behaviors]. Of the remaining seven articles, two were about packet traffic on the darknet and how this traffic sniffing can predict the behavior of users[Che12]. With the detection of user activity on the darknet comes the downside of losing anonymity. These packet sniffing depots also must remain completely hidden, as if a user finds that someone has been spying on their activity, they will conduct a distributed denial of service attack on the relay point. One of the relevant papers was about detecting homemade explosive recipes and marketplaces on the darknet[Kal+16]. Two more of these articles used data mining and machine learning to attempt to predict user activity on the darknet, after mining popular hacking forums for the control set. These papers were called "Exploring and Data Mining the Dark Side of the Web," and "Predicting Hacker Adoption on Darkweb Forums Using Sequential Rule Mining." Because of the dangers of going on the darknet, and the quality content of the articles our search returned, we decided that a systematic review of papers that related to the darknet end-user experience would be the best way to transmit our message. In the end of the paper, we discuss information found in the six most relevant papers. This information is critical to understanding and being safe on the darknet, and our exhaustive search methods have found these four papers to be of good quality. The papers not mentioned in this discussion were only partially related to the end-user experience, and thus to keep our discussion brief and informative they were omitted.

3 METHODS

because of the dangers of the darknet, and the exigence to compile a systematic review of what we know so far, we have tailored three research questions to guide our search. These research questions will steer our literature review towards user-study criteria.

- *RQ1: What are the usage strategies of darknet users?*
- *RQ2: What are the potential risks and vulnerabilities found on the darknet that could jeopordize a users safety?*
- *RQ3: What are the privacy and security concerns of darknet Users?*

Our systematic review is focused on the usage and users of darknet/darkweb. given the nature of the study topic, the papers focused on this research are very limited. Thus, our analysis consists of the database search and title and keyword screening in ACM DL, IEEE Xplore, ScienceDirect, SSRN, Google Scholar and Sage

Journals. Papers were included if they met the following criteria: (1) Published in a **peer-reviewed publication**, (2) Published in **English**, (3) Paper included the**primary human subjects data**, (4) The technology studied was **darkweb/darknet related**. Papers were excluded if: (1) the papers were not full-Papers, which means they were work-in progress, and (2) if the papers full text was not available even after contacting the publication venue or authors.

3.1 Database Search

Our Database search consisted of three levels of screening in order to tailor the search results to our research questions. First, we queried five databases SSRN, IEEE Explore, ACM, Sage Journals and Google Scholar. The search criteria for each of these databases was originally a simple boolean search operation of darknet or darkweb. Using this screening query we gathered 34,554 articles. These articles were not all necessarily relevant, so further keyword, title, abstract and full body analysis was required to further screen these articles. The following methods were found to be the most fruitful queries and screening mechanisms.

3.2 User-Study Screening

To narrow the results further, we conducted a screening using the term user-study. Since this systematic review centers around the end user experience on the darknet, this query clarified which articles were useful. In addition to our original query of darknet or darkweb, each database was searched with an additional Boolean and operation, including the strings ”user study” or ”user studies. While using this method, it is important to note that some outlier articles will be found. For the screening process, the articles were searched for title, abstract, keywords and full body relevance. This means some false positives came up, which had the words user study or user studies in the text but were not actually user studies. Using this further screen we found 177 articles across all five databases. Further research papers will collect articles based only on title and key words, as these databases advance their search functions more comprehensively. Sage Journals, SSRN and Science Direct yielded no results from the user study screening. Google scholar returned the bulk of our results, with ninety-three relevant articles. IEEE found two new results after the user study screen, and these two articles were found to have high quality.

3.3 Manual abstract screening

After user-study screening there were 177 articles remaining. These articles were classified as relevant, borderline and not relevant using the method of manual abstract screening. In this dataset, there were sixteen duplicate articles and seven non-english articles. As stated earlier, this systematic review focuses only on english articles, so these duplicates and foreign language articles were removed from our database. Upon abstract screening, eight articles were found to be relevant, thirteen were found to be borderline, and one hundred and thirty-three were found irrelevant. The relevance criteria was based upon some simple screens. First, the article must be directly related to the darknet. If the article is instead a user study about deep learning, or a different section of the web, it must be excluded. If the article is about the framework of the web, and has nothing to do with the end user, it was excluded. If the article seems to have no bearing on either the user or the darknet / darkweb, it was also excluded and marked as irrelevant.

3.4 Thematic Analysis

The one-hundred thirty three non-relevant articles were deemed irrelevant only if their content had nothing to do with the darknet or peer to peer darknets. IEEE Explore yielded only one irrelevant article. ACM had five irrelevant articles. The majority of irrelevant articles were found on Google scholar, with a whopping 127 irrelevant articles across the database. Of the irrelevant articles, eighteen were found to be related to deep learning, and the neural webs which are present in deep learning. These articles were found because of our query deep web, or our query user study / studies. Although some deep learning articles are relevant to the darknet, these eighteen were not. four more articles were related to data mining, but not relevant to the darknet. Three irrelevant articles were found to be books and not journal articles, so these were removed as they are not relevant to the systematic review, only articles were chosen as relevant. Ten of the irrelevant articles were related to cyber-security, and may have mentioned the darknet once or twice within their body, however these articles were deemed to either have no relevant information about the darknet or no information about the user experience on the darknet.

Irrelevant Articles	
Deep Learning	13%
Data Mining	3%
Books	2%
Cyber-Security	7%
All Other	75%

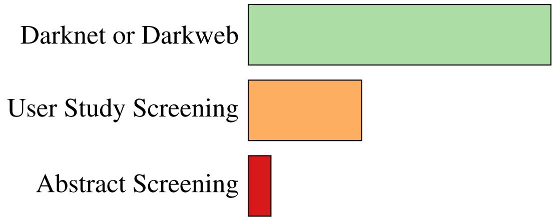
After the irrelevant articles were analyzed, we looked at the borderline articles. These were a step above irrelevant because they either had something to do with the darknet, peer to peer networks, or illegal activity online that the darknet user may come into contact with. Our database search returned thirteen articles that were relevant in one way or the other, but not exactly relevant to our paper. Of these articles, eight were returned from Google scholar, two from IEEE Explore, and two from ACM digital library. Three of the thirteen articles were related to cyber crime and crime prevention. One of the borderline articles was about anonymity on the darknet. Four of these articles were related to the actually networking aspect of the darknet. One of the borderline articles was about homemade explosives on the darknet. Another borderline article was about evaluating text visualization on the darknet. Another article was simply an overview of the research done on the darknet. Another of the borderline articles was about mining key-hackers on the darknet. The last article is about why peer to peer file sharing networks are dangerous.

Borderline Articles	
Cyber Crime	23%
Anonymity	7%
Network Info	30%
Overview	7%
Data Mining (darknet)	7%
Other	16%

3.5 Manual Full-Text screening

In order to further screen these texts, we examined the full body of each paper. Of the eight relevant articles, three were quantitative studies. The remaining five were qualitative studies. Of the ten borderline articles, four were flagged for their content about specific sections of the darkweb, yet none of them were comprehensive articles. These borderline articles helped us to build our systematic review, but at least one portion of the article was deemed to be irrelevant. These articles were excluded from the final discussion because of their half-useful nature.

Relevant Articles	
Quantitative	37%
Qualitative	63%



4 DISCUSSION

4.1 What is The Darknet?

The World Wide Web is a network of linked hypertext files. This web is classified into three regions: the surfaceweb, the deepweb, and the darknet. The surfaceweb is accesible to all users of the internet. This is what you see when you make a Google search, or you browse your favorite body-building forum. The deepweb is the collection of websites that are not indexed by the clearweb, usually because they require authentication. Some examples of deepweb sites are your private Facebook page and feed, the medical records of a patient in a hospital, or a full text PDF of an article found in an academic journal database. Finally, the darknet refers to a collection of pages that are found in an encrypted network. The darknet is specifically designed to keep every user completely anonymous and untraceable. The darknet and its users are the focus of this systematic review.

Creating a platform for anonymity, as you can guess, attracts a very large array of users:

- People who want to conceal their web browsing so they don't feel like they are being spied on by their ISP or their government
- People who want to communicate with online friends without the logs of their chat being saved on a database somewhere
- People who want to publicise journalistic articles without fear of an oppresive regime

However, much of darknet activity is conducted by criminals. Drug markets and forums comprise much of the darknet. Another large section of the darknet is devoted to hackers who test, write and deploy their code from behind the shroud of the darknet[AL20].

4.2 Types of Anonymous Communication on the Darknet

4.3 TOR

The most popular way to access the darknet is through a Firefox shell browser, TOR. TOR is an abbreviation for The Onion Router. Onion routing is the most trusted anonymity system. Grahn et. al explains this process in her paper, ”Anonymous Communication on the Internet.”

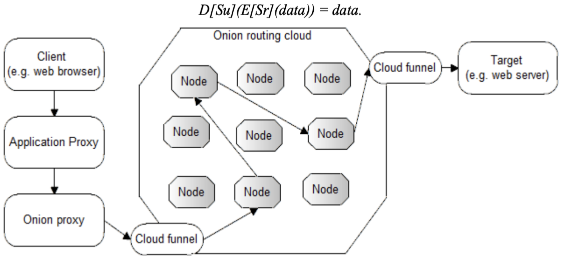


Figure 1: Onion routing cloud with example path.

http://proceedings.informingscience.org/InSITE2014/InSITE14p103-120Grahn0483.pdf

> Repeatedly encrypted messages are sent along an unpredictable route through several network nodes called onion routers. These routers communicate with each other through TCP tunnels. Traffic passes bidirectionally along those circuits with minimal latency. A layer of encryption is removed by each onion router and the message is sent further to the next router. This procedure prevents intermediary nodes from knowing the origin, destination, and contents[GFP14].

Onion routing encrypts the packet in four levels, taking a level of encryption off at each node. This means that even if some node intercepts the packet, it may have to guess at the hash that is used to decrypt the packet. Each packet or cell is five hundred and twelve bytes[DMS04], and consists of a header and a payload. Part of the header contains a circuit id, so that the data can pass through the predefined circuit that was created when the user first opened the TOR browser. There are two types of cells that TOR sends. These cells are diagrammed in the figure below, showing the structure of the control cell and the relay cell respectively:

1. control cells
2. relay cells

2	1	509 bytes
CircID	CMD	DATA

2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA

https://apps.dtic.mil/sti/pdfs/ADA465464.pdf

Control cells are the packets mentioned earlier with the create or destroy command. When the user starts TOR, they send a create command which systematically generates the TOR circuit with the purpose of sending later relay cells which contain the data the user wishes to send. Relay cells carry end-to-end stream data. Relay cells have a header that control cells don’t, called a relay header. The cipher used to encrypt the relay and control cells is called the AES cipher symmetric key cipher[DMS04]. For relay nodes, instead of create and destroy, the commands are as follows:

1. Relay data (for data flowing down the stream)
2. Relay begin (to open a stream)
3. Relay end (to close a stream cleanly)
4. Relay teardown (to close a broken stream)
5. Relay connected (to notify the OP that a relay begin has succeeded)
6. Relay extend and relay extended (to extend the circuit by a hop, and to acknowledge)
7. Relay truncate and relay truncated (to tear down only part of the circuit, and to acknowledge)
8. Relay sendme (used for congestion control)
9. Relay drop (used to implement long-range dummies)

Relay cells are only sent once the circuit is established, otherwise they would be incabable of their end-to-end property. Upon relaying a cell, the onion router looks up the corresponding circuit from the circuitID and then sends the relay cell through the TOR circuit using the private and public keys generated by the circuit. At each level, the node unwraps the header and payload with their session keys. The key is used to sign the cell, and then the key is used to decrypt one layer of the cell. TOR uses symmetric key encryption through its relays. After the circuit is used up, the user sends a destroy command which breaks down the entire circuit. After the destroy command, the user is unable to send any more relay cells through the circuit[DMS04]. Although compromised nodes can expose a user, as long as the compromised node is not the last node the encryption should hold. The following figure explains the encryption and decryption at each layer. The data passes through a tunnel which is TLS encrypted. Typically, port 443 is used for this tunnel[DMS04].

> In onion routing, one circuit was built for each TCP stream, but in TOR, each circuit can be shared by many streams[GFP14].

The difference between TOR and onion routing is important. P2P communication systems use onion routing, but they are not TOR[GFP14]. TOR is the quickest browser that uses onion routing, because each circuit can be shared in many other streams. In P2P communication, the circuits are limited to one data stream.

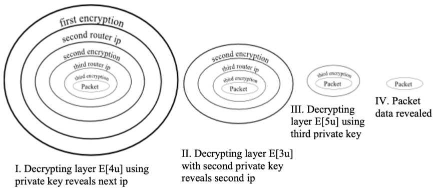

first encryption
second router ip
second encryption
third router ip
third encryption
Packet
I. Decrypting layer E[4u] using private key reveals next ip
II. Decrypting layer E[3u] with second private key reveals second ip
III. Decrypting layer E[5u] using third private key
IV. Packet data revealed

Figure 2: Onion with triple encryption.

http://proceedings.informingscience.org/InSITE2014/InSITE14p103-120Grahn0483.pdf

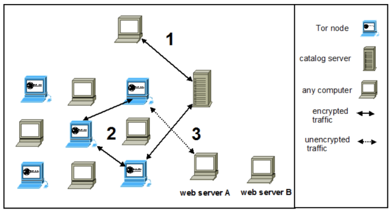


Figure 4: Example connection in TOR.

http://proceedings.informingscience.org/InSITE2014/InSITE14p103-120Grahn0483.pdf

Grahn et al. also does a good job of explaining the artchitecture of a message sent in onion routing.

> A message sent in an onion router architecture contains a virtual circuit identifier, a command (create, destroy, and data), and data. The onion occurs as the data field. A node receiving a create command along with an onion sends another create along with a virtual circuit identifier and the onion to the next node (Goldschlag et al., 1996). If a node receives another command than create, destroy or data a destroy command is sent back through the virtual circuit[GFP14].

The commands are protected under four layers of encryption, so even an important message such as a destroy command is also secure using onion routing. Another important security measure in TOR is that each node knows the predecessor and successor, but they are unaware of all other nodes in the network. TOR boasts this system called perfect forward security. This greatly enhances security, especially if one or more nodes are compromised. Even if a node is compromised, it doesn't know where your data will go after it leaves the successor node. TOR can also detect data congestion and route around it for enhanced speed[DMS04]. TOR also added a function in v2 routing that checks packet integrity from one node to the next. This further ensures that no packets will be decrypted before the exit node. Mixing, padding and traffic shaping are not included in the exit node in the TOR network[DMS04].

To host a site on TOR, the user must have TOR installed and have a web server running locally on the same computer. Once the site is up, TOR configures a public and private key for the server so that traffic can be encrypted[DMS04].

> In the original Onion Routing design, a single hostile node could record traffic and later compromise successive nodes in the circuit and force them to decrypt it. Rather than using a single multiply encrypted data structure (an onion) to lay each circuit, Tor now uses an incremental or telescoping path-building design, where the initiator negotiates session keys with each successive hop in the circuit[DMS04].

As you can see from this quote, the forward navigation of TOR is extremely important. Without the keys from the successor node, the data sent cannot be decrypted by the compromised node.

With these TOR nodes throughout the world, it is almost impossible to breach the user's security. The only time when there is a possibility of anonymity revocation through TOR is if law enforcement or some other party is watching the exit node. Users can tell TOR at any time to choose a new onion circuit if they are concerned their privacy may be compromised.

4.4 Freenet and I2P

Another widely used darknet communication type is anonymous P2P communication. These networks are not as popular as TOR, but they also follow rigorous security measures for their users. One popular anonymous P2P network is called Freenet:

> Freenet (Clarke, Sandberg, Wiley, Hong, 2001) is like a social network, in which files can be anonymously shared, Web pages accessible only through Freenet can be anonymously published and browsed, and anonymous chat forums are available[GFP14].

Many users prefer Freenet for its anonymous chat.
One of these P2P networks is I2P. I2P routers map connections through i2P tunnels. This anonymity is also built on onion routing.

4.5 Darknet Websites

Akintaro et. all sum up darknet markets nicely:

> Dark websites look like any other websites but instead of ending with .com or .edu, they

> usually end with .onion. These sites also use a scrambled naming structure that creates URLs that are often impossible to remember[APM19].

It is possible for darknet merchants to control the first few letters of their onion domain by spamming the domain creation process until the correct letters come up, but all v2 and v3 urls have at least thirty extra characters tacked on to the end which make them impossible to memorize. This makes public key verification of markets and vendors extremely important, as it is common for an imposter site to use the same first characters of the site's domain and change the part of the domain that nobody remembers[APM19]. This specific type of phishing attack is very prevalent on the darknet, and it is part of the reason onion domains are less trustworthy than a .com or .edu. Cryptomarkets are another type of website on the darkweb. These markets employ advanced encryption to protect the user's anonymity in buying goods and services from the darknet.

4.6 Cyber Crime

Cyber crime is not limited to the darknet. A lot of cyber crime is conducted on the clearnet. The darknet is, however, an attractive platform for criminals as it is more difficult to trace their activities and identity on the darknet. In their article, "Darknet and Black Market Activities Against the Cybersecurity: A Survey," Akintaro et. al outlines crime on the darknet. They begin their article by citing three types of crime that occur on the internet:

> 1. Against Person: This type of crime include people harassment using computer, which can be through email, cyber stalking, and pornography and so on.
> 2. Against Property: Crimes includes computer vandalism, possession of unauthorized computer information and unauthorized computer infringement via cyberspace.
> 3. Against Government: This is referred to as cyber terrorism. For example, an individual or group of people illegal access into government website[APM19].

Once again, these crimes are not limited to the darknet. Many criminals are less tech savvy, and commit crimes on the clearnet. The crimes cited most commonly actually occur on the clearnet. Crimes against property and against government are more often found on the darknet, as the repercussions of this type of crime are more severe. Crimes against government are often committed on the darknet, as the shroud of anonymity protects the assailant from the watchful eyes of whatever law enforcement agency is present in their country. Many times government data ends up leaked on the darknet, and then many other criminals can harvest and use this data without having to expose their identities at all. The article then goes on to explain black markets. The authors state that:

> An example of Black Market born because of the expansion of the web is the Darknet. The Darknet is comprised of numerous black-market websites where everyone's identity is veiled against authorities and law enforcement[APM19].

The darknet is not limited to being a black market. As discussed earlier, journalism and other anonymous activities take place in the darknet. A large portion of the darknet, however, is a black market or cryptomarket[AL20]. These markets are tax free and theoretically untraceable.

Another important factor discussed in the article is the rise and fall of darknet markets. One of the first and most popular darknet markets was called Silk Road. Researchers have investigated the spread and quality of darknet drug trafficking on Silk Road specifically, because when it first came out there were not many competitors on the darknet[AL20]. Silk Road was the first publicly known darknet market that allowed personal sized purchases.

> Silk Road was first characterised as an "eBay for Drugs", with drug consumers making personal use-sized purchases, and transactions were described as 'business-to-customers. Just before its closure, more than 1000 vendors were active on Silk Road and annual sales were estimated at 89.7 millions USD[Bro+16].

As you can see from the quote, business at Silk Road was booming. Even though Silk Road was making a lot of money, the actual percentage of darknet market purchased drugs contributes little to the international drug trade[Bro+16]. Later, Silk Road was actually shut down by law enforcement, but with the fall of Silk Road came many more markets, both copycat and unique.

> Even though it [Silk Road] was busted in 2013 by government authorities, many copycat markets were reproduced after[APM19].

Darknet markets compete with street dealers, rather than wholesale entities like drug cartels[APM19]. What's interesting about darknet markets is that their vulnerability to law enforcement shutdowns are nullified sheerly by the property that when one market falls another takes its place. In Broseus et. al paper, they identify the four most popular cryptomarkets in terms of vendors:

- Silk Road 2
- Evolution
- Agora[Bro+16]

Today, only Silk Road 2 remains, in the short time from 2016 until now, two of the three most trusted markets have fallen.

The location of vendors in darknet markets should also matter a lot to the market user. Domestic packages are much less likely to be seized than packages coming in from overseas. This can be troubling, as some goods are nearly impossible to get in the US. High risk vendors will make a large purchase from overseas, and then sell their goods domestically. This diagram shows a breakdown of drug traffic from the three most trusted darknet sites as mentioned earlier

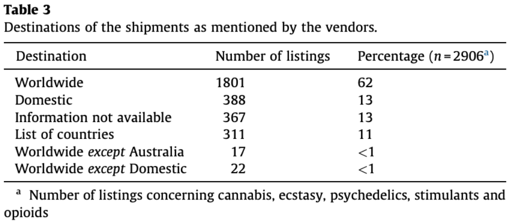


Table 3
Destinations of the shipments as mentioned by the vendors.

Destination	Number of listings	Percentage ($n = 2906$[a])
Worldwide	1801	62
Domestic	388	13
Information not available	367	13
List of countries	311	11
Worldwide *except* Australia	17	<1
Worldwide *except* Domestic	22	<1

[a] Number of listings concerning cannabis, ecstasy, psychedelics, stimulants and opioids

https://pdf.sciencedirectassets.com/271258/

Vendor popularity is very important across markets. Often, new vendors on different markets may try to create a username similar to a trusted vendor to try and take their reputation. In Broseus' article, they analyze vendor names to try and see how many unique vendors are active on the darknet. Sometimes, a vendor may have an account on two different markets with two different names, which makes it even harder to tell who is who[Bro+16]. A popular method for vendor consistency is the use of a PGP signature. This signature is encrypted with the vendor's private key, and only those users who have the vendor's public key can decrypt the message. Signing vendor profiles is the easiest way to verify that a vendor is who they say they are[Bro+16]. An example of what a vendor might post to verify their name and identity is the following:

> ”Formerly BCBUDking on Silk Road and MarijuanaMan39 on Atlantis, BCBUDKING on BMR, Sheepmarket and TORMarket - Pandora - My PGP has not changed it is still me!”[Bro+16].

or

> “Also I have hear someone was pretending to be me on Cannabis Road so always verify its really me with my PGP [. . .] I NEVER CHANGE MY PGP FROM WHATEVER SITE IM ON”[Bro+16].

In the following figure, it is easy to see how important PGP signing is, as each vendor has a few appearances with their key for their name.

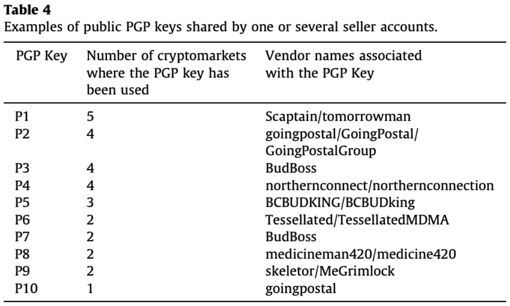


Table 4
Examples of public PGP keys shared by one or several seller accounts.

PGP Key	Number of cryptomarkets where the PGP key has been used	Vendor names associated with the PGP Key
P1	5	Scaptain/tomorrowman
P2	4	goingpostal/GoingPostal/ GoingPostalGroup
P3	4	BudBoss
P4	4	northernconnect/northernconnection
P5	3	BCBUDKING/BCBUDking
P6	2	Tessellated/TessellatedMDMA
P7	2	BudBoss
P8	2	medicineman420/medicine420
P9	2	skeletor/MeGrimlock
P10	1	goingpostal

https://pdf.sciencedirectassets.com/271258/

One factor that goes in to a market's popularity is it's listing on the Reddit analogue Dread. In order to have a Dread page, a market must adhere to the Dread community standards. This means no taboo illegal activities, such as gun sales or child pornography. Many markets change their products in order to advertise and host market discussions on Dread. Customers on the darknet use crypto-currency to hide their purchases. Darknet markets also adopt the policy of third party escrow, where the customer's money is held from the vendor until the vendor delivers the good or service that was promised. Many of the black markets on the darknet have issue insurance, where if the vendor never delivers their product the market foots the cost of the service.

The darknet is also rife with data leaks. This article states that:

> In 2015 a Hacker posted a data dump of 9.7 gigabytes in size which include account details and log-ins for some 32 million users of the social networking site AshleyMadison.com in the Dark web[APM19].

While this leak is not directly related to black markets, as the data was made public for all, it is another factor that explains some of the landscape of the darknet. The darknet allows people who have found vulnerabilities, as with this Ashley Madison site a safe place to reveal their illegal findings. Often, the type of information leaked on the darknet is related to high security topics. The Ashley Madison leak exposed thousands of people to be cheating on their spouses. Often, instead of leaking the information right away, the cyber criminal on the darknet will exact a ransom of the users[APM19]. In exchange for a small sum of money, their personal information will be expunged from the leak.

Interestingly enough, in 2020 there were at least two new domains which even hold the same name as Silk Road. Darknet markets are quick to be shut down, and even quicker to be spun up. Like the Hydra (the namesake of a European darknet site that was shutdown around the same time of Silk Road), when one market shuts down another two take its place. The article goes on to cite the types of cyber crime that are specific to the darkweb:

- Drug, Weapons and Exotic Animal
- Stolen Good and Information
- Murder
- Terrorism
- Illegal Financial Transaction
- The Hidden Wiki[APM19]

Perhaps the most darknet specific and interesting crime is The Hidden Wiki. This database of tips for staying anonymous, how to deal with vendors buying drugs and guns, how to hire someone for murder, etc., is a first resource for many new darknet users.

4.7 Revocation of Anonymity

TOR offers many safety measures for users to maintain anonymity.

> Since communication might be encrypted, endpoints can be revealed, and may expose who is behind the communication. By allowing anyone to join and leave the TOR network at any time while also onion routing is used, it is impossible to spy on all nodes in the network[GFP14]

This joining, leaving, and regeneration of circuits is one of TOR's biggest safety features. In "Addressing Anonymous Ab uses: Measuring the Effects of Technical Mechanisms on Reported User Behaviours," Ahmad et. al conducted a user study using five methods of anonymity revocation specifically to target criminals who abuse the darknet. Two of these revocation schemes were from trusted third parties such as Cloudflare. Two more schemes involved access limitations by service providers. The last revocation scheme involved blocking activity with the consent of a trusted third party. In this paper, the goal was to revoke anonymity of criminals, while still allowing freedom of speech and discussion to continue encrypted and uninterrupted. Spam and phishing were the two main illegal activities targeted, while illegal communications and illegal reporting on censored topics were deemed acceptable, as freedom of speech allows. The study was conducted as an online survey, where participants were randomly assigned to groups. The participants were asked whether or not they were bothered by the potential revocation of their anonymity should they be flagged for criminal activity. Many users stated that yes, this was a breach of darknet safety. The problem with privacy revocation is that authoritarian regimes may abuse this power[AL20].

4.8 Threats Against TOR

TOR is vulnerable to timing attacks, where assailants can identify which TOR nodes are communicating with each other.

> The general idea in TOR has been to protect against learning between which nodes there is communication, not to protect against confirmation if two nodes are communicating[GFP14]

One way that the article suggests to protect from malicious nodes in the TOR network is to build a list of trusted nodes, and only use these trusted nodes in your TOR circuit. Another way to protect from malicious nodes is to rebuild your circuit a few times, while hopefully this shuffle can give a better chance of reliable nodes[GFP14]. Browser based attacks are also prevalent in TOR, where a node in the network misrepresents its network traffic capacity. The author suggests:

> To prevent browser based attacks users have to make sure that extensions are not allowed in the browser they are using. If a user uses the standard TOR bundle and runs the program from a virtual machine that is reset after each execution of the program, then the browser based attack should be avoided[GFP14].

This quote underlines the importance of both using a VPN and also a virtual machine to access the darknet. It is possible to access the darknet without either of these precautions, but if a user plans to do risky activity these measures must be taken for safety.

4.8.1 Tracking and Prediction

In addition to revoking anonymity, many parties attempt to monitor darknet users' activity, even without exposing their names. This type of attack on anonymity is a passive attack, the goal is to observe and then take action accordingly. Tor does its best to combat this attack using public key cryptography:

> To avoid traffic capturing TOR uses Diffie-Hellman key exchange between the onion proxy and each circuit router for the duration of a circuit's lifetime[GFP14].

"In A Study of Packet Sampling Methods for Protecting Sensors Deployed on Darknet" Narita et. al examines the process of monitoring malicious activities on the internet by intercepting darknet packets. This system:

> analyzes captured malicious packets and provides effective information for protecting good internet users from malicious activities[Nar+16].

If, for example, a phishing scheme can be observed by intercepting the phishers packet, they can try to figure out how to mitigate this attack in the future. The monitoring system consists of many sensors deployed in unused IP space on the internet. The packets that come from the darknet are assumed to be malicious, and thus these are the packets that they try to capture. Should a darknet user uncover the packet sniffer at the random IP address, they will probably attack it with a DoS attack[Nar+16].

4.8.2 Predicting Criminal Hacking Activity by Mining Darknet Forums

Another way that people attempt to predict darknet activity is by analyzing prior activity and using this model to predict what will happen in the future. In "Predicting Hacker Adoption on Darkweb Forums," Marin et. al creates a framework for predicting the actions of darknet hackers who are active on hacking forums. In this paper, more than 330,000 hacker posts on a popular darkweb forum were used as the training set. Next, the model is split into a set of rules where the rule x implies the result y. Using these rules, security analysts can respond to future attacks with confidence[MSS18].

5 CONCLUSION

This study investigates the darknet from the perspective of the users. The darknet is an ever growing community of anonymous users which lays unreachable by surface web browsers. To use the darknet, one must employ onion routing, using TOR, Freenet, or I2P peer to peer networks. The reasons someone may wish to stay anonymous on the internet are boundless. Whether the user is attempting to publish a journal article in a fascist regime, or whether the user plans to buy drugs and alcohol to be delivered to their house, the darknet provides a platform to do so.

The landscape of the darknet is vast, with forums, markets, chatroom's and link directories scattered around. To maintain anonymity the darknet user must choose the domains and activities they conduct carefully, as someone may well be watching them. In this paper we learned about revocation of anonymity schemes, which is perhaps one of the greatest threats which is facing darknet users. As a user of the darknet, the safe assumption is that somone is always trying to track, monitor and predict your activity. This underlines the importance of proper TOR, VPN and PGP or other types of encryption. It also drives home the point of choosing the proper cryptocurrency for transactions in the darknet. Users would do well to adopt the less track-able Monero, as opposed to bitcoin which must be scrambled and wallet addresses can still be figured out by threat actors against the darknet user (which may be law enforcement.) It is unclear which of these revocation methods will be adopted going forward. The scariest methods to revoke anonymity come from breaking the exit node security and mined prediction algorithms. Since users can leave and enter TOR at any time, the packet analysis is less dangerous for users. These packets often require additional cracking as unless they are reaching the exit node, they may have one or more layers of encryption around them. Compromised onion nodes do pose a threat to users, but as they are found and destroyed this threat is less pressing.

If, on the other hand, law enforcement can profile a user on a forum and predict where and what they may post next, it is easy to compromise their whole account. In summary, we glance once again at the research questions we set out to answer with this paper.

- *RQ1: What are the usage strategies of darknet users?*
- *RQ2: What are the potential risks and vulnerabilities found on the darknet that could jeopordize a users safety?*
- *RQ3: What are the privacy and security concerns of darknet Users?*

The usage strategies of darknet users are vast, but are primarily related to using the TOR network to:

- buy
- chat
- post
- research

The darknet can be a difficult place to forge a reputation in if the user has no technical experience. To access the best forums and markets, there is often a programming or hacking test required to gain membership. Another way to gain membership to these forums that doesn't require technical skill is no network and message with some of the users on the market or forum. These users can give what is essentially a voucher to the user, and they can use this voucher to create a premium membership.

Another way the darknet is less accesible to the user is the credit system. Lots of darknet sites use a credit system. Credits are given to the users who post, comment or conduct other activity on the forum. With these credits, the market user can then purchase data leaks, premium forum sections and other clout related items. The main risks and vulnerabilities on the darknet are those who would wish to revoke your anonymity.

Another risk to using the darknet is interacting with criminals, drug users, and illegal vendors. Although most of these criminals will have trouble getting the personal information of the user, they can still run scamming schemes and attempt to phish data.

Darknet markets go up and fall down so often that it is often detrimental for users and vendors alike. One of the. most popular ways to get scammed on a darknet market is the ”exit scam.” With an exit scam, the administrators of the market take all the money from vendor accounts and user accounts and head for the hills, as the market is erased from the darknet forever. Empire market, one of the biggest markets in 2020 exit scammed, even thought they were widely believed to be the most trusted markets. Other darknet markets such as BitBazaar and Square market also exit scammed in 2020. When dealing with criminals, it is important to keep your wits about you and avoid putting too much money in your vendor or user account, as the exit scam is always a possibility. As for the privacy and security concerns of the darknet user, users should always be using a vpn within a virtual machine. This both eliminates the TOR exit node vulnerability and protects the users computer from spyware, malware and ransomware that may be accidentally downloaded while browsing the darknet.

So much of our lives during this era of the global COVID-19 pandemic are online. To be a responsible web user, we believe that a strong comprehension of the surfaceweb, deepweb, and darknet are important to understand the digital landscape of our world. This paper summarizes the research done so far so that the reader can understand the darknet without having to take the leap into actually going on the darknet. Many guides have been written on safety on the darknet, for example in the popular darknet forum and Reddit analogue Dread, the subdread operation security (opsec) has many resources available. The darknetmarkets subdread is also worth reading if you are going to go on the darknet.

References

[DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. “Tor: The Second-Generation Onion Router”. In: (2004). DOI: `10.21236/ada465464`.

[Che12] Hsinchun Chen. “Dark Web Research Overview”. In: *Dark Web: Exploring and Data Mining the Dark Side of the Web*. New York, NY: Springer New York, 2012, pp. 3–18. ISBN: 978-1-4614-1557-2. DOI: `10.1007/978-1-4614-1557-2_1`. URL: `https://doi.org/10.1007/978-1-4614-1557-2_1`.

[GFP14] Kaj J Grahn, Thomas Forss, and Göran Pulkkis. “Anonymous communication on the internet”. In: *Proceedings of Informing Science & IT Education Conference (InSITE)*. 2014, pp. 103–120.

[Bro+16] J. Broséus et al. “Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective”. In: *Forensic Science International* 264 (2016). Special Issue on the 7th European Academy of Forensic Science Conference, pp. 7–14. ISSN: 0379-0738. DOI: `https://doi.org/10.1016/j.forsciint.2016.02.045`. URL: `https://www.sciencedirect.com/science/article/pii/S0379073816300676`.

[Kal+16] George Kalpakis et al. “Interactive Discovery and Retrieval of Web Resources Containing Home Made Explosive Recipes”. In: *Human Aspects of Information Security, Privacy, and Trust*. Ed. by Theo Tryfonas. Cham: Springer International Publishing, 2016, pp. 221–233. ISBN: 978-3-319-39381-0.

[Nar+16] M. Narita et al. “A Study of Packet Sampling Methods for Protecting Sensors Deployed on Darknet”. In: *2016 19th International Conference on Network-Based Information Systems (NBiS)*. 2016, pp. 76–83. DOI: `10.1109/NBiS.2016.37`.

[MSS18] E. Marin, J. Shakarian, and P. Shakarian. “Mining Key-Hackers on Darkweb Forums”. In: *2018 1st International Conference on Data Intelligence and Security (ICDIS)*. 2018, pp. 73–80. DOI: `10.1109/ICDIS.2018.00018`.

[APM19] Mojolaoluwa Akintaro, Teddy Pare, and Akalanka Mailewa. “Darknet and black market activities against the cybersecurity: A Survey”. In: Apr. 2019.

[AL20] Wajeeha Ahmad and Ilaria Liccardi. “Addressing Anonymous Abuses: Measuring the Effects of Technical Mechanisms on Reported User Behaviors”. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI ’20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–14. ISBN: 9781450367080. DOI: `10.1145/3313831.3376690`. URL: `https://doi.org/10.1145/3313831.3376690`.