DARK WEB

Pevekar Zainab Ashfaque , Abis Husain Parvez Natiq.
Department of computer engineering.
A.I.Abdul Razzak Kalsekar Polytechnic, Panvel.

Abstract: ***The layers of the Internet go far beyond the surface content that many can easily access in their daily searches. The other content is that of the Deep Web, content that has not been indexed by traditional search engines such as Google. The furthest corners of the Deep Web, segments known as the Dark Web, contain content that has been intentionally concealed. The Dark Web may be used for legitimate purposes as well as to conceal criminal or otherwise malicious activities. It is the exploitation of the Dark Web for illegal practices that has garnered the interest of officials and policymakers.***

Individuals can access the Dark Web by using special software such as Tor (short for The Onion Router). Tor relies upon a network of volunteer computers to route users' web traffic through a series of other users' computers such that the traffic cannot be traced to the original user. Some developers have created tools—such as Tor2web—that may allow individuals access to Torhosted content without downloading and installing the Tor software, though accessing the Dark Web through these means does not anonymize activity. Once on the Dark Web, users often navigate it through directories such as the "Hidden Wiki," which organizes sites by category, similar to Wikipedia. Individuals can also search the Dark Web with search engines, which may be broad, searching across the Deep Web, or more specific, searching for contraband like illicit drugs, guns, or counterfeit money. While on the Dark Web, individuals may communicate through means such as secure email, web chats, or personal messaging hosted on Tor. Though tools such as Tor aim to anonymize content and activity, researchers and security experts are constantly developing means by which certain hidden services or individuals could be identified or "deanonymized."

Anonymizing services such as Tor have been used for legal and illegal activities ranging from maintaining privacy to selling illegal goods—mainly purchased with Bitcoin or other digital currencies. They may be used to circumvent censorship, access blocked content, or maintain the privacy of sensitive communications or business plans. However, a range of malicious actors, from criminals to terrorists to state-sponsored spies, can also leverage cyberspace and the Dark Web can serve as a forum for conversation, coordination, and action. It is unclear how much of the Dark Web is dedicated to serving a particular illicit market at any one time, and, because of the anonymity of services such as Tor, it is even further unclear how much traffic is actually flowing to any given site.

Keywords: Dark web, Thor, deanonymized.

Introduction:

Beyond the Internet content that many can easily access online lies another layer—indeed a much larger layer of material that is not accessed through a traditional online search. As experts have noted, "searching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore, missed."1 This deep area of the Internet, or the Deep Web, is characterized by the unknown—unknown breadth, depth, content, and users.

The furthest corners of the Deep Web, known as the Dark Web, contain content that has been intentionally concealed. The Dark Web may be accessed both for legitimate purposes and to conceal criminal or otherwise malicious activities. It is the exploitation of the Dark Web for illegal practices that has garnered the interest of officials and policymakers. Take for instance the Silk Road one of the most notorious sites formerly located on the Dark Web. The Silk Road was an online global bazaar for illicit services and contraband, mainly drugs. Vendors of these illegal substances were located in more than 10 countries around the world, and contraband goods and services were provided to more than 100,000 buyers.4 It has been estimated that the Silk Road generated about $1.2 billion in sales between January 2011 and September 2013, after which it was dismantled by federal agents. The use of the Internet, and in particular the Dark Web, for malicious activities has led policymakers to question whether law enforcement and other officials have sufficient tools to combat the illicit activities that might flow through this underworld. This report illuminates information on the various layers of the Internet, with a particular focus on the Dark Web. It discusses both legitimate and illicit uses of the Dark Web, including how the government may rely upon it. Throughout, the report raises issues that policymakers may consider as they explore means to curb malicious activity online.

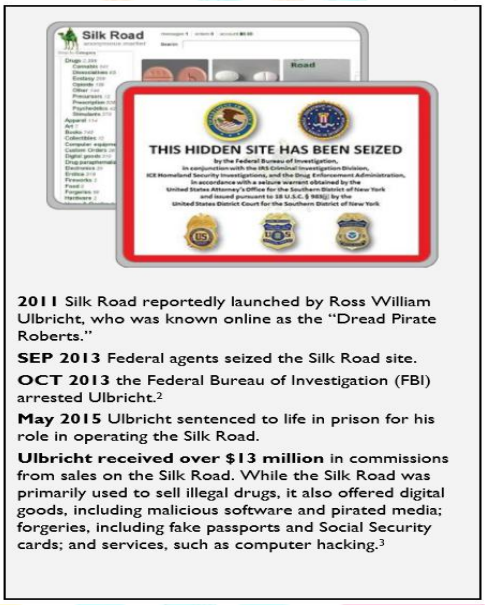

Fig:1

Layers of the Internet

Many may consider the Internet and World Wide Web (web) to be synonymous; they are not. Rather, the web is one portion of the Internet, and a medium through which information may be accessed. In conceptualizing the web, some may view it as consisting solely of the websites accessible through a traditional search engine such as Google. However, this content known as the "Surface Web" is only one portion of the web. The Deep Web refers to "a class of content on the Internet that, for various technical reasons, is not indexed by search engines," and thus would not be accessible through a traditional search engine.8 Information on the Deep Web includes content on private intranets (internal networks such as those at corporations, government agencies, or universities), commercial databases like

Lexis Nexis or Westlaw, or sites that produce content via search queries or forms. Going even further into the web, the Dark Web is the segment of the Deep Web that has been intentionally hidden. The Dark Web is a general term that describes hidden Internet sites that users cannot access without using special software. While the content of these sites may be accessed, the publishers of these sites are concealed. Users access the Dark Web with the expectation of being able to share information and/or files with little risk of detection.

In 2005, the number of Internet users reached 1 billion worldwide. This number surpassed 2 billion in 2010 and crested over 3 billion in 2014. As of July 2016, more than 46% of the world population was connected to the Internet. While data exist on the number of Internet users, data on the number of users accessing the various layers of the web and on the breadth of these layers are less clear.

Surface Web: The magnitude of the web is growing. According to one estimate, there were 334.6 million Internet top-level domain names registered globally during the second quarter of 2016. This is a 12.9% increase from the number of domain names registered during the same period in 2015. As of February 2017, there were estimated to be more than 1.154 billion websites. As researchers have noted, however, these numbers "only hint at the size of the Web," as numbers of users and websites are constantly fluctuating.

Deep Web: The Deep Web, as noted, cannot be accessed by traditional search engines because the content in this layer of the web is not indexed. Information here is not "static and linked to other pages" as is information on the Surface Web. As researchers have noted, "it's almost impossible to measure the size of the Deep Web. While some early estimates put the size of the Deep Web at 4,000 to 5,000 times larger than the surface web, the changing dynamic of how information is accessed and presented means that the Deep Web is growing exponentially and at a rate that defies quantification."

Dark Web: Within the Deep Web, the Dark Web is also growing as new tools make it easier to navigate. Because individuals may access the Dark Web assuming little risk of detection, they may use this arena for a variety of legal and illegal activities. It is unclear, however, how much of the Deep Web is taken up by Dark Web content and how much of the Dark Web is used for legal or illegal activities.

Fg:2

Accessing and Navigating the Dark Web

The Dark Web can be reached through decentralized, anonymized nodes on a number of networks including Tor (short for The Onion Router) or I2P (Invisible Internet Project). Tor, which was initially released as The Onion Routing project in 2002,19 was originally created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online. Tor "refers both to the software that you install on your computer to run Tor and the network of computers that manages Tor connections."20 Tor's users connect to websites "through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy." Users route their web traffic through other users' computers such that the traffic cannot be traced to the original user. Tor essentially establishes layers (like layers of an onion) and routes traffic through those layers to conceal users' identities. To get from layer to layer, Tor has established "relays" on computers around the world through which information passes. Information is encrypted between relays, and "all Tor traffic passes through at least three relays before it reaches its destination." The final relay is called the "exit relay," and the IP address of this relay is viewed as the source of the Tor traffic. When using Tor software, users' IP addresses remain hidden. As such, it appears that the connection to any given website "is coming from the IP address of a Tor exit relay, which can be anywhere in the world." While data on the magnitude of the Deep Web and Dark Web and how they relate to the Surface Web are not clear, data on Tor users do exist. According to metrics from the Tor Project, the mean number of daily Tor users in the United States across the first two months of 2017 was 353,753— or 19.2% of total mean daily Tor users. The United States has the largest number of mean daily Tor users, followed by Russia (11.9%), Germany (9.9%), and United Arab Emirates (9.2%).

Communicating On (and About) the Dark Web

There are several different ways to communicate about the Dark Web. One of the first places individuals may turn is Reddit. There are several subreddits pertaining to the Dark Web, such as Dark Net Markets, Deep Web, or Tor. These

forums often provide links to sites within the Dark Web. Reddit provides a public platform for Dark Web users to discuss different aspects of the Tor. It is not encrypted or anonymous, as users who wish to engage in forum discussion must create an account. Individuals who wish to use a more secure form of communication may choose to utilize email, web chats, or personal messaging hosted on Tor: Email service providers, for instance, typically only require users to input a username and password to sign up. In addition, email service providers generally offer anonymous messaging and encrypted storage. A number of anonymous, real-time chat rooms such as The Hub and Onion Chat are hosted on Tor. Feeds are organized by topic. While some sites do not require any information from users before participating in chats, others require a user to register with an email address. Personal messaging, through Tor Messenger, is another option for Tor users who wish to communicate with an added layer of anonymity. Bitmessage is a popular messaging system which offers encryption and strong authentication. Decentralized, peer-to-peer instant messaging systems, such as Ricochet, also run on Tor and allow for anonymized communication. Specific vendor sites may host private messaging as well.

Is the Dark Web Anonymous?

Guaranteed anonymity is not fool proof. While tools such as Tor aim to anonymize content and activity, researchers and security experts are constantly developing means by which certain hidden services or individuals could be identified or "deanonymized." For example, in October 2011 the "hacktivist" collective Anonymous, through its Operation Darknet, crashed a website hosting service called Freedom Hosting operating on the Tor network which was reportedly home to more than 40 child pornography websites. Among these websites was Lolita City, cited as one of the largest child pornography sites with over 100GB of data. Anonymous had "matched the digital fingerprints of links on [Lolita City] to Freedom Hosting" and then launched a Distributed Denial of Service (DDoS) attack against Freedom Hosting. In addition, through Operation Darknet, Anonymous leaked the user database—including username, membership time, and number of images uploaded—for over 1,500 Lolita City members. In 2013, the Federal Bureau of Investigation (FBI), reportedly took control of Freedom Hosting and infected it with "custom malware designed to identify visitors." Since 2002, the FBI has supposedly been using some form of a "computer and internet protocol address verifier" consistent with the malware in the Freedom Hosting takeover to "identify suspects who are disguising their location using proxy servers or anonymity services, like Tor." In February 2017, hackers purportedly affiliated with Anonymous took down Freedom Hosting II a website hosting provider on the dark web that was stood up after the original Freedom Hosting was shut down in 2013. Hackers claimed that over 50% of the content on Freedom Hosting was related to child pornography. Website data were dumped, some of which may now identify users of these sites. Of note, security researchers estimated that Freedom Hosting II housed 1,500–2,000 hidden services (about 15-20% of their estimated number of active sites). The FBI conducted an investigation into a child pornography website known as Playpen, which was operating on the Dark Web and had nearly 215,000 members. In 2015, Virginia District Court judge authorized a search warrant allowing law enforcement to employ a

network investigative technique to try to identify actual IP addresses of computers used to access Playpen. Through the use of the NIT, the FBI was able to uncover about 1,300 IP addresses and subsequently trace those to individuals. Criminal charges have been filed against more than 185 individuals.

Why Anonymize Activity?

A number of reasons have been cited why individuals might use services such as Tor to anonymize online activity. Anonymizing services have been used for legal and illegal activities ranging from keeping sensitive communications private to selling illegal drugs. Of note, while a wide range of legitimate uses of Tor exist, much of the research on and concern surrounding anonymizing services involves their use for illegal activities. As such, the bulk of this section focuses on the illegal activities.

Online Privacy Tor is used to secure the privacy of activities and communications in a number of realms. Privacy advocates generally promote the use of Tor and similar software to maintain free speech, privacy, and anonymity. There are several examples of how it might be used for these purposes: Anti-Censorship and Political Activism. Tor may be used as a "censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content." Because individuals may rely upon Tor to access content that may be blocked in certain parts of the world, some governments have reportedly suggested tightening regulations around using Tor. Some have purportedly blocked access to it at times. Political dissidents may also use Tor to secure and anonymize their communications and locations, as they have reportedly done in dissident movements in Iran and Egypt. Sensitive Communication. Tor may also be used by individuals who want to access chat rooms and other forums for sensitive communications both for personal and business uses. Individuals may seek out a safe haven for discussing private issues such as victimization or physical or mental illnesses. They may also use Tor to protect their children online by concealing the IP addresses of children's activities. Businesses may use it to protect their projects and help prevent spies from gaining a competitive advantage.

Leaked Information. Journalists may use Tor for communicating "more safely with whistle blowers and dissidents." The New Yorker's Strongbox, for instance, is accessible through Tor and allows individuals to communicate and share documents anonymously with the publication. In addition, Edward Snowden reportedly used Tails (an "operating system optimized for anonymity") which automatically runs Tor to communicate with journalists and leak classified information on U.S. mass surveillance programs. Among the documents leaked by Snowden was a top-secret presentation outlining National Security Agency (NSA) efforts to exploit the Tor browser and de-anonymize users.

Illegal Activity and the Dark Web

Just as nefarious activity can occur through the Surface Web, it can also occur on the Deep Web and Dark Web. A range of malicious actors leverage cyberspace, from criminals to terrorists to state-sponsored spies. The web can serve as a forum for conversation, coordination, and action. Specifically, they may rely upon the Dark Web to help

carry out their activities with reduced risk of detection. While this section focuses on criminals operating in cyberspace, the issues raised are certainly applicable to other categories of malicious actors. Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations. For instance, criminals can easily leverage the Internet to carry out traditional crimes such as distributing illicit drugs and sex trafficking. In addition, they exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft. The FBI considers high-tech crimes to be among the most significant crimes confronting the United States. The Dark Web has been cited as facilitating a wide variety of crimes. Illicit goods such as drugs, weapons, exotic animals, and stolen goods and information are all sold for profit. There are gambling sites, thieves and assassins for hire, and troves of child pornography. Data on the prevalence of these Dark Web sites, however, are lacking. Tor estimates that only about 1.5% of Tor users visit hidden services/Dark Web pages. The actual percentage of these that serve a particular illicit market at any one time is unclear, and it is even less clear how much Tor traffic is going to any given site. One study from the University of Portsmouth examined Tor traffic to hidden services. Researchers "ran 40 'relay' computers in the Tor network which allowed them to assemble an unprecedented collection of data about the total number of Tor hidden services online about 45,000 at any given time and how much traffic flowed to them." While about 2% of the Tor hidden service websites identified were sites that researchers deemed related to child abuse, 83% of the visits to hidden services sites were to these child abuse sites "just a small number of pedophilia sites account for the majority of Dark Web http traffic." As has been noted, however, there are a number of variables that may have influenced the results. Another study from King's College London scanned hidden services on the Tor network. Starting with two popular Dark Web search engines, Ahmia and Onion City, they used a web crawler to identify 5,205 live websites. Of these 5,205 websites, researchers identified content on about half (2,723) and classified them by the nature of the content. Researchers determined that 1,547 sites contained illicit content. This is a sample of websites on hidden services in Tor; the researchers' crawler accessed about 300,000 websites (including 205,000 unique pages) on the network of Tor hidden services. Of note, in 2015 Tor estimated that there were about 30,000 hidden services that "announce themselves to the Tor network every day." Further, Tor estimated that "hidden service traffic is about 3.4% of total Tor traffic." More recent data from March 2016 to March 2017 indicate that there were generally between 50,000 and 60,000 hidden services, or unique .onion addresses, daily. The Dark Web can play a number of roles in malicious activity. As noted, it can serve as a forum through chat rooms and communication services for planning and coordinating crimes. For instance, there have been reports that some of those engaged in tax-refund fraud discussed techniques on the Dark Web. The Dark Web can also provide a platform for criminals to sell illegal or stolen goods. Take the role of the Dark Web in data breaches, for example Malware used in large-scale data breaches to capture unencrypted credit and debit card information has been purchased on the Dark Web. One form of malware, RAM scrapers, can be purchased and remotely installed on point-off sale systems, as was done in the 2013 Target breach, among others. Thieves can sell stolen information for profit on the Dark Web. For instance, within weeks of the

Target breach, the underground black markets were reportedly "flooded" with the stolen credit and debit card account information, "selling in batches of one million cards and going for anywhere from $20 to more than $100 per card." Such "card shops" are just one example of the specialty markets on the Dark Web. Not only can data be stolen and sold through the Dark Web, it can happen quickly. In one experiment by security vendor BitGlass, researchers created a treasure trove of fake "stolen" data including over 1,500 names, social security numbers, credit card numbers, and more. They then planted these data on DropBox and seven well-known black market sites. Within 12 days, the data had been viewed nearly 1,100 times across 22 countries. Cybercriminals can victimize individuals and organizations alike, and they can do so without regard for borders. How criminals exploit borders is a perennial challenge for law enforcement, particularly as the concept of borders and boundaries has evolved.

Payment on the Dark Web

Bitcoin is the currency often used in transactions on the Dark Web. It is a decentralized digital currency that uses anonymous, peer-to-peer transactions. Individuals generally obtain bitcoins by accepting them as payment, exchanging them for traditional currency, or "mining" them. When a bitcoin is used in a financial transaction, the transaction is recorded in a public ledger, called the block chain. The information recorded in the block chain is the bitcoin addresses of the sender and recipient. An address does not uniquely identify any particular bitcoin; rather, the address merely identifies a particular transaction. Users' addresses are associated with and stored in a wallet. The wallet contains an individual's private key, which is a secret number that allows that individual to spend bitcoins from the corresponding wallet, similar to a password. The address for a transaction and a cryptographic signature are used to verify transactions. The wallet and private key are not recorded in the public ledger; this is where Bitcoin usage has heightened privacy. Wallets may be hosted on the web, by software for a desktop or mobile device, or on a hardware device.

Government Use of the Dark Web

Because of the anonymity provided by Tor and other software such as I2P, the Dark Web can be a playground for nefarious actors online. As noted, however, there are a number of areas in which the study and use of the Dark Web may provide benefits. This is true not only for citizens and businesses seeking online privacy, but also for certain government sectors namely the law enforcement, military, and intelligence communities.

Conclusion

As we know that the deep web is expanding exponentially, so is the darknet which is giving way to enormous illegal activities providing platform, which is forcing the law enforcing agencies to use new unorthodox methods to track these technologically savvy criminals. These software are frequently used by whistle blowers, journalists, military and even terrorist organizations to access a secure channel for communication. Virtual currency which is used in dark market transactions is termed as Bitcoins. It is a very secure and flawless way of carrying out e-business. No one can be completely anonymous on internet but software such as TOR, free net and I2P make it extremely strenuous to

track its clients. This gives them freedom from censorship, privacy, a secure channel to communicate. The future of Deep Web includes much more secured and improvised darknet, more power and well established market places for darknet, gauging information will become easier, tracking down of Bitcoins that is the currency of dark markets will become harder and moreover, with increase in awareness among people will result in more users of darknet and simultaneous expansion of the same.

References

[1] Christopher. Web Crawling The Stanford University Info lab Foundations And Trendsr In Information Retrieval Vol 4 .Web Crawling.

[2] Sherman, C., & Price G. (2001).. Medford, NJ: Cyber Age Books, Information Today. The invisible web: Uncovering information sources search engines can't see. [3] Bergman, M. (2001).Presented by Mat Kelly,CS895 – Web-based Information Retrieval, Old Dominion University,Septmber27, 2011.The deep web: Surfacing hidden value.

[4] Daniel Sui, James Caverlee, Dakota Rudesill. A Wilson Center Publication The Deep Web and The Dark Net: A Look Inside The Internet's Massive Black Box.