THE DARK WEB:

The Elusive Playground for Crime and Anonymity

By Ian Pascoe

Introduction

To most, the dark web is daunting. It is elusive, mysterious and dangerous. This virtual "location" is rarely explored by the average internet user. The dark web resides in a place where most browsers cannot reach. It requires special software configurations and sometimes special authorization to access. Often mistaken for the deep web, the dark web is a small portion of the deep web that is not indexed by search engines like Google or Bing. These networks are so hidden, and the users are granted so much anonymity, that it allows for a vast amount of illegal activity to occur. These crimes include illegal transactions on crypto-markets, which sell and broker transactions of narcotics, counterfeit money, forged documents, stolen credit card information, unlicensed pharmaceuticals, weapons and other illegal goods. One of the most infamous drug trafficking sites on the dark web was the Silk Road, which was ultimately shut down in 2013, after already being shut down in the past. Other crimes on the dark web include fraud and bitcoin scams like proxying or onion cloning. There are also plenty of myths construed about the dark web by internet users, based commonly on the situations conjured by Hollywood. Sites displaying live torture, or offering bounties on high-profile individuals, are often a scam, and will not be upkept or advertised on the dark web. These crimes and myths all contribute to the fear that is often associated with the dark web and will be discussed in-depth.

What is the Dark Web?

As stated, previously, the dark web requires a lot of additional software, knowledge, and experience to reach. Unlike the "clear web" which we all know and (most) love, the network that comprises the deep web (parent entity of the dark web) consists of mostly machine-to-machine communication and data distributing. Therefore, it cannot be indexed by search engines. Similarly, the dark web uses this machine-to-machine communication on a large scale called the Tor (The Onion Router) network. This network is comprised of a giant network of volunteer computers to route users' web traffic in such a complex way that the traffic of data cannot be traced back to the original source. Some third parties have created software such as Tor2web that allow individuals to access Tor network content without downloading full Tor browsing software. This does not provide to the same anonymity as the full software, which has left many users vulnerable to attack or prosecution. Accessing these dark web sites takes some serious technical research and persistence. It also doesn't hurt to contact some of members (if possible) for advice on connecting (Korolov).

What is done on the dark web is invisible due to the architecture of the Tor network. Users tend to have something to hide, seeking anonymity while making transactions. It is obvious why criminals have chosen this network as their playground for crime. The anonymity on these sites have allowed for several marketplaces to flourish and be extremely profitable. One of these marketplaces is the Silk Road, which will be discussed more in-depth later on. These markets sell a wide variety of illegal products that include but are not limited to: stolen credit card information, stolen identification information, narcotics, pornography (more specifically child pornography), services that include hacking, assassination or robbery, and lastly malware, which could be zero-day exploits (discussed later), spyware, adware, ransomware, etc. These products are bought using untraceable cryptocurrencies to further mask their crimes. The only products currently traceable by law enforcement are narcotics, assassination and robbery because there is a real-life footprint left behind by the perpetrators. The rest of the products can be completely transferred digitally, which with Tor is completely anonymous making them impossible to trace as of now.

Tor also has vulnerabilities, however. It is possible for law enforcement to run their own Tor relays to monitor the flow of traffic entering and exiting the Tor network (Bradbury).

Bradbury also goes on to explain, “Roger Dingledine, the director of the Tor project, points out that the authorities could just as easily monitor Internet communications with the complicity of major ISPs, which would enable them to watch those communicating with Tor nodes before their traffic reached the dark web, or after it left.” This would essentially strip the anonymity from the Tor network for those short periods of time before and after connecting.

Tor is not the only dark web technology, either. Freenet is an older project that allows users to store files on each other’s computers and create ‘freesites’, accessible only through that network. I2P is similar to Tor, where websites are hosted anonymously (Bradbury). Whonix is an anonymous web browsing tool that was made specifically for Linux, and even more specifically made for use on virtual machines which protects the user’s computer from attack if things were to go wrong while surfing the dark web. Yandex, a Russian technology developer, created Yandex browser, which lets the user surf anonymously and also scans websites for files that are trying to steal personal information. When looking at a similar issue, other countries are looking to create their own internets. China and even Iran have investigated creating their own internets that could be looked at as though they are dark webs. This is only because they are to be compartmentalized segments of traditional internet, similar to the layer that is the dark web (Bradbury). These technologies could be created for several reasons. They could be used just to separate their country’s internet users from others, or to keep other countries’ users out.

While experts are still uncovering new information and vulnerabilities with the dark web, there is still much to be learned about. There are plenty of good theories behind cracking the crimes performed on the dark web, but law enforcement still relies heavily on human error to lead them to the criminals. Until there is a way to crack the anonymity on the dark web technologies, the thwarting of criminals is still going to be a slow and painful process.

Past Issues and Potential Solutions

The most notorious crypto-market on the dark web is the Silk Road, supposedly established in 2011 by Ross William Ulbricht. Ulbricht started with extremely humble beginnings. At age 26, he grew magic mushrooms and had no good way of selling them. Being rather savvy in technology for an individual at the time, Ulbricht created a simple website on a tucked away portion of the internet. The dark web was much less of a conversation in 2011, so no one really noticed when he started accepting the cryptocurrency bitcoin for his magic mushrooms, that he would effortlessly send through the mail (Tarnoff).

After quickly depleting his crop of magic mushrooms, Ulbricht began to allow other users onto his site to sell other drugs, while taking a small percentage of each sale. These drugs ranged from marijuana all the way to opioids. While this took him out of the hot seat for drug possession, he was now a broker for online drug sales. This means he was connecting buyers and sellers, and effectively becoming the middle man for thousands of illegal transactions. This effectively doubled his profits, but it also linked him to a huge amount of illegal activity in which officials were now hot on the trail (Tarnoff). It should also be noted that the Silk Road increased the variety of its products over time. By the time Ulbricht was arrested, the site was offering primarily drugs, but also offered malicious software, pirated media, forgeries, and services like computer hacking (Tarnoff). As anyone can imagine, the government put a large target on this market, making its downfall a top priority.

Ulbricht’s ultimate demise was leaving an enormous paper trail (Tarnoff). The technology in which he used was flawless, he, however, was not. Officials were eventually able to uncover several conversations he had with his employees. They uncovered talks of how to improve gaps in security on the website, dilemmas with salesmen and the commission rate, and Ulbricht calling for hitmen to kill subordinates that had betrayed him. In 2013, Ulbricht was arrested for receiving over $13 million in commission for sales on his website. By 2015, prosecution found him guilty and he was sentenced to a life in prison for his role in operating the Silk Road (Tarnoff). While these products are the most commonly seen on the dark web, there was one that was specifically excluded by the Silk Road, most likely due to Ulbricht's morals.

Pornography, more specifically child pornography is a highly sought-after product on the dark web. Studies conducted on the Gnutella P2P utility (a dark web search and response site) showed that 1.6% of searches and 2.4% of responses were related to child pornography material. This study also dove deeper into discovering that the users that were accessing this material were using Gnutella strictly for this exchange (O'Brien 247). Tor provides the perfect platform for trading these images and videos. Buyers are provided complete anonymity and seller sites can provide masked download links that law enforcement officials struggle to trace. The issue with this exchange is that the legislation about pornography varies widely throughout different cultures.

US legislation in section 63 of the Criminal Justice and Immigration Act 2008 criminalized "extreme pornographic images" defined as "grossly offensive" or "disgusting" (O'Brien 249). Inevitably, the interpretation of this legislation can vary. Disgusting and grossly offensive first needs to be agreed upon before doing so. Fortunately, most of the world has agreed that pornography showing children fit these illegal descriptions. Recently, prosecutors are formulating new ways to police the internet for these breaches of law. The UK has attempted sending lists of suspected child porn sites to internet service providers. Other third parties, such as the 'hacktivist' group Anonymous, were able to remove a few instances of child porn on the dark web, replacing the links with those to denial of service attacks, which effectively shut down the servers hosting these images (O'Brien 252). While this is a great triumph for law enforcement, these efforts are few and far between and will hopefully become more common as experience and knowledge of the dark web grows.

Besides the actual crimes that occur on the dark web, there are also issues plaguing law enforcement on how to legally prosecute these criminals. Traditional investigative methods include extensive steps when information is out of US jurisdiction. This requires informal law enforcement cooperation mechanisms be used to obtain this information. This usually begins with investigation of a supposed perpetrator's email address and IP address. This is used to find the location of the device being used, in which law enforcement looks to seize this device. If the device is out of jurisdiction, then investigators must use consent-based cross-border evidence collection methods (Ghappour 1093). This doesn't even incorporate dark web tunneling.

If the perpetrator were to use the dark web to anonymize, law enforcement would have to trace the IP through the Tor server all the way to their actual IP address, which is currently not possible. Tor would show one of the proxy computers' IP address, rendering this information useless to prosecutors (Ghappour 1095). Fortunately, as knowledge of these systems grow, there are new tactics being developed to investigate these crimes.

Hacking is becoming law enforcement's key instrument in finding these criminals. Using network investigative techniques, an investigator can reach a computer without knowing its actual physical location. They use virtual pathways from computers and bridges between networks to trace activity to the perpetrator's IP address. Using malware and these techniques, law enforcement has been able to turn the perpetrators computer into a surveillance device, in turn, helping prosecute the criminals (Ghappour 1096). While all of this sounds easy on paper, it is quite the task to execute. Host computers can have a variety of different security layers to pass through before being able to distribute the malware, making this method of investigation a work in progress.

Results of Interview

During a short interview I conducted with Mark D. Matulaitis, my previous High School Senior Project Mentor, I gained a firsthand perspective from someone in the field of Computer Engineering. Although he does not work directly on projects regarding the dark web, Mark has worked at Intel for over 25 years, where he works in close quarters with several digital security experts. His genuine interest in security technology has also driven him to do research on the dark web, having read several books and articles on the topic.

When asked for his opinion on the future of the dark web after The Silk Road and other crumbling online drug markets, Mark went on to explain that he believes the future of the dark web is going to mainly consist of "Digital Arms Trade". Digital arms trade is the distribution of a large variety of virus source code on the dark web. These viruses could be bought in these crypto-markets using bitcoin and other crypto-currencies as compensation, similar to narcotics and other products. It goes without saying that these products being sold on the web are extremely dangerous and allows for a large distribution of these viruses across the globe. Mark went on to list the various types of viruses and malware that were being dispersed in this trade, stating that it included but was not limited to spyware, adware, ransomware, and viruses that could live strictly in your computers register so that they were extremely hard to find, and even harder to remove. He emphasized that these were not even the worst exploits to be sold on the dark web. Zero-day exploits are also making their way onto these markeplaces.

Zero-day exploits are intrusion techniques for which no software patch currently exists. Therefore, these exploits are extremely dangerous, effective and hard to recover from, once becoming a victim. Mark informed me that, luckily, this extreme form of digital arms trade is still generally new to the dark web, with only a few known zero day exploits available for sale in small, unpopular marketplaces. One marketplace, however is making its mark on the dark web as "the place" to get zero-day exploits. "TheRealDeal Market" has begun to emerge in the dark web as a place where anyone can go to get digital armaments. Mark says that while other marketplaces sell digital armaments, TheRealDeal Market prides itself in being the one-stop-shop for highly sought after zero-day source code, even offering zero-day hacking services from a highly trained and knowledgeable hacker if you don't have the skills to do it yourself.

Mr. Matulaitis believes that this is the future of the dark web markets because these products offers the highest reward for the risk. A zero-day exploit when used against the right victim can offer a huge return on investment for the person who buys them, whether this be money extracted from an online account, credit card information of a victim or just crucial information on a person that may even give the user an unfair advantage in a political campaign. Mark says that drug trade on the dark web is flawed because there will always be the exchange of the actual product that can be intercepted by law. With the anonymity of Tor, digital armaments can be traded completely anonymously on the network, currently without a trace. This is terrifying to think about and is exactly why Mark Matulaitis has such a realistic fear and assumption that it will be the next predominant business model on the dark web.

My Comments

In my opinion, the dark web is looked at as much more of a boogeyman than an actual threat to the average user. A vast majority of internet users will never encounter the dark web. Only 1.5% of Tor users even access the dark web (Ward). To the average user, the dark web is something you are taught to stay away from if you want to stay safe. While this is true, there are still hundreds of thousands of people that browse the dark web every day. Unfortunately for some, critical personal information can be the product sold on these sites. Due to this and other reasons such as drug trafficking and child imagery, law enforcement is obligated to look into stopping criminals from prospering on this platform.

There are also many benefits to using a Tor network. Online anonymity is something rare and has a lot of value to many of its users. Many human rights activists use anonymous IP addresses on Tor networks to blog about important issues (NPR). There are many legal uses of Tor that millions of users take advantage of on a daily basis as well. Many people use it to protect their privacy while browsing. An example would be e-book collections of subversive works that are available on the Dark Web, away from government censors. There are also sites set up specifically for journalists to share files and stories. These sites serve as an important pipeline that reporters can use to smuggle out important stories that portray authoritarian regimes in a negative light. Finally, there are secure image-sharing sites that offer ordinary citizens an additional layer of privacy when sharing sensitive photos. All these uses may be perfectly legal and understandable, but the reality remains that they only account for a portion of Dark Web traffic. Much of the traffic on the Dark Web is illegal. (Sui, Caverlee, Rudesill)

The only thing that I disagree with in these paraphrases is that these legal uses of Tor should be referenced under the entity of the “Deep Web”. The term “Dark Web” should be coined to any illegal activities that occur on the deep web. The legal activities that occur on the deep web are actually quite liberating. Anyone can share their opinions of controversial topics without any fear of repercussions. Some users that have received recognition for this are, Chelsea Manning, Julian Assange, and Edward Snowden, who exposed their governments for unethical practices. While these may be controversial, it truly streamlines and helps condone free speech that some people may not even have bothered to share if they could not be under the cloak of a Tor Network.

The big controversy for law makers in regards to the dark web is how to regulate these anonymizing technologies so that illegal activity is few and far between. The dark web could not exist without the concept of anonymous web browsing, so first they would have to regulate Tor. Already, law makers would have to find a way of regulating it so that it does not destroy the benefits that Tor provides for its users. Using Tor is not a crime, and there is no clear way to distinguish the criminals from the innocent users. This makes the potential actions by lawmakers drastic. The only real way to prevent ALL crimes on the dark web is to prohibit the use of anonymous technologies on the web. Another huge obstacle is the international reach of the dark web. Policies regarding the dark web need to be clear and agreeable by all international parties, which would be an incredible task to accomplish. There have been several countries that have attempted to regulate Tor. China has tried to ban Tor use, Russia has tried to deanonymize Tor for political reasons, and Australia has attempted to halt Tor traffic within its borders. All of these have been, as you can imagine, unsuccessful. But this enforces the fact that coming to an international agreement on Tor is nearly impossible.

Overall, I believe that anonymity will be impossible to regulate because individuals will never be willing to voluntarily sacrifice this right just to eliminate all crime on the dark web. Anonymity is already extremely rare as it is. It has become common knowledge that if you are on a network, someone is capable of tracking you. Tor is one of the few exceptions, which is why it has become such a valuable resource for some people. Instead, law enforcement is going to be forced to learn how to unmask users on Tor in order to prosecute criminals. Currently, there is no clear way of doing this, but law enforcement has been developing theories on how to do so.

Summary

Many people have heard of the dark web and the crimes that occur on this platform, but not many people understand how it works. Without a Tor browser an individual with the desire to access the dark web would not even be able to do so. Using Tor takes experience, not to mention finding the links to unindexed websites. While crimes are often the highlight of activity on the deep web there are many other legal uses of the deep web that go on without much notice. Anonymity while on the web seems like something of a myth to most internet users, but with Tor web surfers can explore and write information without a traceable identity. In a world where privacy is becoming less and less common, this can be extremely valuable. Cases like that of Edward Snowden have shown people that their data, while on the surface network, is always traceable. This enforces the value of anonymous web browsing. The major issue here is how to unmask that anonymity when it is being used to do something illegal. There are already several theories on how to exploit Tor for justice, but there is not clear and concise way of tracking someone using Tor as evidence in a court of law. Successful efforts have been few and far between, still depending mainly on human error to give law enforcement the information it needs for prosecution. But with persistence and more experience, law enforcement will steadily improve its network investigative techniques so that perpetrators will be traceable even with the mask of Tor, to which a new anonymity tool will most likely erect, but that is an issue for the future.

Sources

Bradbury, Danny. “Unveiling the Dark Web.” Network Security, vol. 2014, no. 4, 2014, pp. 14–17.

Ghappour, Ahmed. "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web." Stanford law review 69.4 (2017): 1075-136. ProQuest. Web. 19 Nov. 2018.

Korolov, Maria. “The Dark Web.” Independent Banker, vol. 66, no. 12, 2016, p. 69.

Matulaitis, Mark D. Interview. 23 Nov. 2018.

O'Brien, Mark. “The Internet, Child Pornography and Cloud Computing: the Dark Side of the Web?” Information &Amp; Communications Technology Law, vol. 23, no. 3, 2014, pp. 238–255.

Sui, D., J. Caverlee, and D. Rudesill. “The Deep Web and the Darknet.” 2015. Web. 19 Nov. 2018.

Staff, NPR. “Going Dark: The Internet Behind The Internet.” NPR, 25 May 2014, Web. 19 Nov. 2018

Tarnoff, Ben. "The Dark Web's Dark Prince; the Silk Road was an Illicit eBay, an Online Marketplace Where You could Buy Drugs, Weapons, Vials of Cyanide--Even Human Kidneys. Ben Tarnoff Reviews "American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road" by Nick Bilton." Wall Street Journal (Online), Jun 12 2017, ProQuest. Web. 19 Nov. 2018 .

Ward, M. “Tor’s Most Visited Hidden Sites Host Child Abuse Images.” 2014, Web. 19 Nov. 2018.