Crimes committed through the dark web

Crimesof the Dark Web

Abstract

Beyond the regular world of the all-accessibleInternet, lies a world of hidden platforms and communities used by only thedarkest and most sinister of individuals. This hidden creation is called theDark Web (DW). The Dark Web is a platform on the internet that is onlyaccessible using a specific type of software. This software allows people tohide behind various IP addresses to remain undetected in order to completeillegal and extremist acts. This paper serves to go into detail about what theDW is and how it is used, what types of crimes are committed, and other illegalacts performed within it. It will explain the different domains that residewithin the DW, what they are used for, and why they were so successful. Thispaper will also go into what kinds of individuals choose to use it, and whythey feel the need to do so, and how they have been caught and stopped in thepast. This paper will strive to cover all different aspects of the DW and all thatis associated with it, to better understand its reason for existing.

Crimesof the Dark Web

There are many types of crimes committedin this world, however the most recently evolved platform for crime is known asthe Dark Web (DW). The DW is a discrete online infrastructure used bymiscreants such as terrorists, where they are able to share their ideologiesand communicate with one another in often illegal activities (Chen, Chung, Qin, Reid, Sageman, & Weimann, 2008). The DW is the main support of crimestaking place in today’s cyberspace, and according to Alrwais, Li, Wang, Xie, andYu, (2013),

these crimes cause hundreds of millions in damage every year. Thereis still limited knowledge about DW infrastructures, despite progress beingmade to understand and disrupt the malignant activities (Alrwais, et al., 2013), though we do know from accounts of experience, as well as the littleresearch that has been done, some of the happenings within DW social networks. This paper will serve to explain the DW, what it is used for, and the differentdomains associated with it. It will go into detail about how individuals accessit, and the different reasons one might have to do so. This paper will alsocover different domains within DW platforms, misconceptions about it, andvarious crimes committed associated with DW use.

What is the Dark Web and how is it accessed?

There are many differentexplanations used to define the DW, as it is something very difficult tounderstand. What is mainly understood about it is, the DW is a class of contenton the internet that is part of something called the “ Deep Web” (Chertoff &Simon, 2015). The Deep Web is a platform that is not available by standardsearch engines, meaning you cannot access it without the correct software(Gehl, 2014). Chertoff and Simon (2015) explain that the DW is used for near-completeanonymity to perform illegal acts away from the face of the public. Accordingto some, the DW is a platform used for power and freedom, attempting toovercome growing social networking as well as state oppression (Gehl, 2014). Toothers, it is a place that is able to foster new opportunities for individualswith malicious intent to commit crimes and “ dark business” in a more secretivefashion (Alrwais, et al., 2013). As mentioned before, it is impossible to enterthe DW without proper software. There are different ways to be able to accessthe DW, but one of

the most common ways is by use of “ The Onion Router,” alsoknown as “ TOR” (Hayes, Cappa, & Cardon, 2018). The Onion Router is aninfrastructure that can be used to create almost completely anonymousconnections over a public domain, which is how individuals roam around the DWand utilize different internet services without being detected (Goldschlag, Reed, & Syverson, 1999). The Onion Router “ covers your online tracks byblending your internet traffic into data from many servers worldwide to makeyou functionally invisible” (Hodson, 2014). The Onion Router was first createdabout 20 years ago as a military research project. Its original intention wasto avoid traffic analysis (TA), which is used to identify IP addresses (Forte, 2006). The individuals running this research project lost control of thesoftware, ultimately making it available to the general public, creatingprivacy on the internet that is almost impossible to control (Forte, 2006). Thereason for this software being called an “ onion” router, is likely due to thelayers involved in it, starting with the all-accessible “ surface web,” andmoving deeper and deeper through layers into the DW (Weimann, 2016). It wasMichael K. Bergman that stated the DW as compared to skimming a net across thesurface of the ocean. You may catch a great deal within the net, however thereis a breadth of information that resides deeper that cannot be reached(Weimann, 2015).

Who is using the Dark Web and Why?

To many, the DW is a terrifyingplace that should never be entered. As most people are aware, it is full ofdangerous individuals, seeking out antisocial activities with others who sharesimilar ideals and interests. The creation of the DW has allowed forindividuals such as terrorists to reside within it

undetected to go about theirbusiness. It is known that these terrorists have been active in public onlineplatforms since the late 1990s, however would get shut down bycounter-terrorism agencies. This is when then DW came in handy for theseindividuals, as the DW provides a kind of security that nowhere else is able toprovide, and therefore is perfect to execute antisocial and illegal acts(Weimann, 2016). A recent study was conducted and found that 57% of the contentresiding within the DW consists of illegal content such as pornography, illicitfinances, drug hubs, weapons trafficking, counterfeit currency, terrorist communication, and more (Moore & Rid). The DW is a host for marketplaces that allow“ vendors” to sell illegal items to consumers using Bitcoin rather than actualmoney (Hayes, et al., 2018). Bitcoin is a crypto-currency that allows for theseseller’s to anonymously trade illegal items on the DW without leaving a trail(Hayes, et al., 2018). It is believed that the DW marketplaces are sosuccessful because consumers of these illegal items feel safe shopping there, because they can be almost certain they will never be caught due to the heftyprecautions used within these sites (Hayes, et al., 2018). This high level ofanonymity nurtures illegal activities within the DW including not only drugtrafficking, but also credit card fraud and identity theft, as well as leaks ofsensitive information (Chertoff & Simon, 2015).

There are various different groupsof people that use the DW for their own personal gain, many of them beingextremist or terrorist groups. One of the first major hate-sites thatoriginated on the DW was a groups of neo-Nazi’s (Anwar & Abulaish, 2012). As of 2012, the neo-Nazi hate-site contained 58 different forums with a totalof 619, 634 threads and over 8 million posts

(Anwar & Abulaish, 2012). Evidenceof these hate groups show the danger that is growing on DW forums, and thesignificant threat they pose to society. Accessibility to these extremistgroups allow for a global audience to be present and share ideals world-widewith one another, that would not be able to be accomplished otherwise (Zhou, Reid, Qin, Chen, & Lai, 2005). Being online means hate groups can now growlarger than ever before. Not only can extremist ideals now reach entirecommunities in the real world, but those communities can now spread theirideals thousands of times faster and join with other communities across theworld, allowing for a much bigger problem than we have ever faced before. Aquote taken from Roversi (2006) states quite literally what is happening in theworld due to these extreme terrorist groups residing on the DW. The quote readsas a testimony against the DW and its happenings of nostalgia for the Fascistera, videos appearing on extremist web sites of police and political “ adversaries,” and propaganda being created against Blacks, gays, and Jews. The statement continues, arguing a complete “ Balkanization” of the web slowly occurring (Roversi, 2006). Balkanization being a fragmentation of the internet that is hostile towards oneanother.

The DW and its users have grownexponentially over the years. In 2007 alone, there was an estimated eighthundred active right-wing websites document in the US (Caiani & Parenti, 2009). As Caiani and Parenti (2009) point out, it is not just the number ofextremist websites on the DW that is interesting, however it is the role theinternet plays in these organizations that is gaining scientific interest. Asresearch expands in this field, there are findings indicating the use of thesesites being dissemination of propaganda,

inciting violence, facilitaterecruitment in order to reach a larger, more global audience, and to connectwith others that have similar interests (Caiani & parenti, 2009). To provefurther this usage of the DW, after the attacks in November of 2015 in Paris, ISIS turned to the DW to spread propaganda in an attempt to protect itssupporters (Weimann, 2016). ISIS's media outlet is known as *Al-Hayat Media Center,* where informationis spread about the happenings within the group, allowing for people from allcorners of the earth to reach and be informed of this growing terroristorganization (Weimann, 2016).

Researchers are still unsure aboutwhether or not the ability to communicate secretly online is a causal factorfor an increase in terrorism. It is known however, that this onlineaccessibility substantially improves the ability of extremist groups to growand prosper, with the capacity to reach a mass audience (Caiani & Parenti, 2009). It is clear that socially unacceptable activities are infinitely easierto execute within the DW than anywhere else, and it makes complete sense whygroups such as ISIS would choose to turn to a platform such as this.

Domains within the Dark Web

As stated before, there are many differentdomains that reside outside as well as within the DW, one being known as theSilk Road (Lacson & Jones, 2016). The Silk Road was a cryptomarket that ledto the popularity of DW marketplaces after its rise and fall between 2011 and2013 (Hayes, et al. 2018). The Silk Road marketplace, throughout its nearly twoyears of operation, generated millions of dollars in revenue for those using it(Lacson

& Jones, 2016). This platform was used mainly for drug dealers andbuyers on an international level. The Silk Road was founded by a mysteriousindividual known as the “ Dread Pirate Roberts,” and used web-based currencylike bitcoin, supported military-grade privacy, and managed to stay out of theeyes of law enforcement everywhere for the two years it remained in use (Lacson& Jones, 2018). As stated before, sites like this are only accessiblethrough the TOR browser, also known as The Onion Router, where URLs alwaysconsisted of seemingly random sets of characters, always followed by “. onion”(Lacson & Jones, 2018). It seems as though the “. onion” was yet anothersecurity feature among the many encryptions already in place. There was a studyconducted by Maddox, Barratt, Allen, and Lenton (2015), in which theyanonymously interviewed users of the Silk Road after its closure in 2013. Theirstudy found that the Silk Road was not just used for buying and selling drugs, but it was also a place that supported personal freedom where open and safediscussions were able to be had regarding stigmatized and illegal behaviorsbetween individuals who shared similar ideologies and interests (Maddox, Barratt, Allen, & Lenton, 2015). This private domain was a place wherepeople could go to avoid public scrutiny and feel like part of a community.

Along with the Silk Road, there arealso other domains and websites within the DW. The Assassination Market websiteis yet another platform that allows individuals to perform illegal acts. Thisplatform is a prediction market where a party will place a bet on the date theybelieve a given individual will die. Whoever guesses accurately collects apayoff (Chertoff & Simon, 2015). Though this website is a predictionmarket, it provides incentive for the

gamblers to assassinate the givenindividual in order to win the large sum of money (Chertoff & Simon, 2015). There are also websites that allow individuals to hire assassins, one being *White Wolves,* and another known as *C'thuthlu* (Chertoff & Simon, 2015). Alongside the Assassination Market, come other websites such as *Banker & Co.* and *InstaCard,* which are websites on the DWthat facilitate untraceable financial transactions using bitcoins or ananonymous debit card issued by a bank (Chertoff & Simon, 2015). Thesewebsites also allow individuals to buy stolen credit card information, one inparticular called *Atlantic Carding* offersthis service (Chertoff & Simon, 2015). With these websites, it has neverbeen easier to buy and sell illegal items on the internet.

Conclusion

Among all of the crimes committed inthe world, those committed on the DW can be considered all the more dangerous. Thisbeing said, we must note that virtual crime is no different than crime in thereal world. All that has changed is the medium to which people are utilizing tocommit these crimes, and the breadth of people that can be reached at any giventime (Chertoff & Simon, 2015). As discovered throughout this paper, the DWis a platform on the internet that allows for near complete anonymity on theweb. This created a world for criminals to be able to exist in communitiescommitting antisocial acts virtually unnoticed by the vast majority of peopleon and off the internet. It also allows for criminals to be able to reach amuch larger audience than ever before, creating a large problem when it comesto terrorist and extremist groups, as well as the buying and selling of illegalitems. This paper served to explore the DW and all it entails, from what it is, to how it was

created, to how to access it, as well as various reasons peoplefeel the need for such a destructive and hateful platform. There is stillongoing research regarding this topic, and much yet to be discovered about theDW. Despite this, it is believed we have a good grasp on this concept from a scientificstandpoint, and will continue to strive to shut down the operations andhappenings on the DW. As we continue this goal, researchers will continue tostudy and monitor different presences on the DW, both for scientific gain, andto ensure the safety of the public.

References

- Alrwais, S., Li, Z., Wang, X., Xie, Y., F. (2013). Finding the linchpins of the Dark Web: a study on topologically dedicated hosts on malicious web infrastructures. *2013 IEEE Symposium on Security and Privacy,* 112-126. DOI: 10. 1109/SP. 2013. 18
- Anwar, T., & Abulaish, M. (2012). Identifying cliques in Dark Web forums – An agglomerative clustering approach. *Intelligence and Security Informatics,* 1-4. DOI: 10. 1109/ISI. 2012. 6284289
- Caiani, M., & Parenti, L. (2009). The dark side of the Web: Italian right-wing extremist groups and the internet. *South European Society and Polotics, 14* (3), 273-294. DOI: 10. 1080/13608740903342491
- Cappa, F., Cardon, J., & Hayes, D. R. (2018). A framework for more effective Dark Web marketplace investigations. *Information, 9* (8), 1-17.
- Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark web: A case study of Jihad on the web.

Journal of the Association for Information Science and Technology, 59 (8), 1347-1359.

- Chertoff, M., & Simon, T. (2015). *The impact of the dark web on internet governance and cyber security.* Waterloo, ON: Centre for International Governance Innovation and Chatham House.
- Forte, D. (2006). Advances in onion routing: description and backtracking/investigation problems. *Digital Investigation, 3* (2), 85-88.
- Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media and Society 18* (7), 1219-1235.
- Goldschlag, D., Reed, M., & Syverson, P. (February, 1999). Onion routing. *Communications of the ACM, 42* (2), 39-41. Retrieved fromhttps://dl. acm. org/citation. cfm? id= 293443
- Hodson, H. (March, 2014). Invisible: A visitors' guide to the dark web. *New Scientist.* Retrieved fromhttps://www. newscientist. com/article/mg22129611-100-invisible-a-visitors-guide-to-the-dark-web/
- Lacson, W., & Jones, B. (2016). The 21 st century DarkNet market: Lessons from the fall of Silk Road. *International Journal of Cyber Criminology, 10* (1), 40-61. DOI: 10. 5281/zenodo. 58521
- Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2015). Constructive activism in the Dark Web: Cryptomarkets and illicit drugs in the digital ' demimonde.' *Information, Communication & Society, 19* (1), 111-126.
- Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy, 58* (1), 7-38.

- Roversi, A. (2006). *L’odio in rete: siti ultras, nazifascismo online, jihad elettronica* , *167,* Il mulino.
- Weimann, G. (2015). Going dark: Terrorism on the Dark Web. *Studies in Conflict and Terrorism, 39* (3), 195-206.
- Weimann, G. (2016). Terrorist Migration to the Dark Web. *Terrorism Research Institute, 10* (3), 40-44.
- Zhou, Y., Reid, E., Qin, J., Chen, H., & Lai, G. (2005). US domestic extremist groups on the Web: link and content analysis. *IEEE Intelligent Systems, 20* (5), 44-51.