DARKNET AND BLACK MARKET ACTIVITIES AGAINST THE CYBERSECURITY: A SURVEY

Mojolaoluwa Akintaro
Department of Information Assurance
St. Cloud State University
St Cloud, MN 56301, USA
maakintaro@stcloudstate.edu

Teddy Pare
Department of Information Assurance
St. Cloud State University
St Cloud, MN 56301, USA
pate1301@stcloudstate.edu

Akalanka Mailewa Dissanayaka
Department of Computer Science and Information Technology
St. Cloud State University
St Cloud, MN 56301, USA
amailewa@stcloudstate.edu

Abstract

The "Dark Web" is a term that alludes explicitly to an accumulation of sites that exist on an encrypted system and can't be found by utilizing customary web crawlers or visited by utilizing conventional programs. Practically all sites on the purported dark web shroud their identity utilizing the Tor encryption tool. The emergence of the dark web has led to a huge increase in malicious activities conducted on the internet such as money laundering, drug trafficking, child abuse, murder and so on. This has negatively affected the effectiveness of cybersecurity. The aim of cybersecurity is to protect information system and data from unauthorized access by hacker and also prevent illegal activities on the internet. This paper describes the different forms of cybercrime carried out on the surface web, impact of black market on cybersecurity, cybercrimes in the dark web and how to monitor the dark web.

Keywords: Cybersecurity, Black-Market, Dark-Web, Cybercrime, Hacking, Hijacking, Computer-Security, Ethics-in-Computing, Security, Threats, Attacks, Vulnerabilities.

1. INTRODUCTION

The creation of the world, wide, web and other search engines such as Google has made easy to access to information anytime. Most of these information easily accessible are on the surface web which is easily accessible through normal search engine [1]. On the other hand, there are some websites that are not easy of access using normal standard search engines since the data embedded on these websites are heavily encrypted. Likewise, these websites called also dark web are very similar to black markets, since the main reason of their creation is to bypass taxes and laws and trade in dangerous illegal goods. As a result, we observe nowadays that black markets also expanded online where a pool of cybercriminals can make a lot of money by selling or exchanging data, buying forbidden data, or goods that are prohibited by government's regulations [2]. So, the emergence of these online black market has affected deeply the effectiveness of cybersecurity and internet governance since people and business are getting more affected by these activities while cybercriminal are rendered more difficult to catch and prosecuted.

2. CYBERSECURITY

Cybersecurity is referred to as the process of protecting computer, software, hardware, data, information, computer network from unauthorized access and alteration by hacker, terrorist and cybercriminals. The Internet established a mean of conducting business, buying and selling of products and services, financial transaction and communication with customers. There are many benefits of using Internet, which include worldwide business advertisement with little or no fee and less man effort within a short period of time. As the use of Internet offers numerous benefits, it also offers equal avenue for hackers, cybercriminal and Terrorists [3] [4].

Cybercrime implies to criminal activities involving the use if Internet, computer and any other type of IT Infrastructure. Cybercrime are in three categories which are [5]:

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

2.1 FORMS OF CYBERCRIME

This section presents the different forms of cybercrime as follows:

- Intellectual Property Theft

Intellectual Property is a new employed model with an economic value. Patents, video and music copyright, trademark are used to protect intellectual property. Attackers tends to target organization internal business information. Examples of Internal business information includes product price list, product design, list of customers etc [3].

- Salami Attack

The act of stealing little amount of money from different bank account which later amounts to a huge money is referred to as Salami Attack. This act is commonly conducted by cybercriminal. In most cases, Salami attack goes unnoticed because the amount deducted are ridiculously small. For example, an attacker develops a software that deduct (50 cents, a month) from several accounts holders in a bank. Majority of the customer would not take note.

- Phishing

This type of attack is conducted via email. The aim is to steal personal and financial information. In this attack, the attacker sends an email appearing to come from a legimate address requesting for user's private information such as username and password, social security number, credit card details etc [3] [6].

- Identity Theft

This is a fraudulent act, in which a cybercriminal steals someone else identity and commit crime with the stolen identity. The type of identity often are name, home address, card number and social security number. Also, with the stolen information such as username & password, bank account details cybercriminal cam access the bank account and make money transfer to another account or make purchase [7].

- Spoofing

This is a process of gaining unauthorized access to computer. In this technique, an attacker manipulates a hosted IP packet and transmit the message whereas the receiver believes to have received the message from a trusted source.

- DOS & DDOS

Denial of Service (DOS) attack interrupts network services whereby making network resources unavailable to authorized users. A Distributed Denial of Service (DDOS) is a DOS attack that spreads malicious content from more than one infected system at the same time. The targeted software are controlled remotely by "Botnets" [3] [6] [7].

2.2 TRENDS IMPACTING CYBERSECURITY

This section describes the few trends impacting cybersecurity as follows:

- Web Application

There have been an increase of attack on web application. Web application require high level of protection as cybercriminal uses these platform to steal data. It is of importance to use a safe browser when conducting important transaction on the internet [5].

- Cloud Application

Majority of companies are migrating into the cloud. The use of cloud computing poses a threat to cybersecurity. As the use of cloud application increases, effective control of cloud services is needed to prevent the loss of sensitive information. Cloud computing offers numerous opportunities so also does the security concerns around it increases.

- Advanced Persistent Threat

This is a new approach of cybercrime. Attacker gain unauthorized access to computer network and remains unnoticed for a period of time. IPS & web application filtering are used to detect such attacks but as attackers keeps improving their techniques. It is important to integrate network security with other security services in order to detect and prevent more advanced threats in the future [5] [7].

3. BLACK MARKET

The black Market can be defined as an Illegal, free market expanding in economies where goods are scanty or heavily taxed [8]. It is basically a clandestine market that takes place outside any government regulations or sanctions to avoid price control and taxes. These markets also called Shadow markets are places where one can purchases assets or any kind of property that are not publicly accessible [9]. There is a motto saying that “No good deed is done in the dark”. A prime example of it is the Black Market. In a nutshell, the main reason for trading through the channel of Black market is to trade contraband, avoid paying heavy taxes and being under the influence of price fluctuations. Likewise, participants in a black can freely exchange stolen or corrupt good without being under the scrutiny of any kind of federal agents or regulations [10]. Since participation in black market activity is considered illegal, each member tries to hide their identity from the government by using cash for example to not leave any footprints during transactions.

According to the Research Institute for Arts and Humanities, the early 2000s saw the growth of cybercrime message forums like ShadowCrew, counterfeitlibrary.com and the Russian language carderplanet.com operating on the clear web through a message board, with members communicating through a Virtual Private Network (VPN) [11].

4. THE DARKNET

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. Recent years have seen dramatic increases in the darknet's aggregate bandwidth, usability, size of shared library, and availability of search engines [11]. To be able to access these websites, participants need to be computer-proficient enough to install the special software required by the black markets' websites. Moreover, the Darknet use complicated encryption techniques to hide people identities and bounce the network traffic around many servers around the world making tracing impossible.

Likewise, Pseudonyms are used for messaging and most transaction like in the Black-Market use Bitcoin and the service of escrow third party for trading. As a result, the surfers and the publishers are anonymous and not easy to catch by investigators. On these websites, Narcotics, Firearms, stolen credit cards numbers, human trafficking, illegal pornography, money laundering services, and even hiring assassins are some of the marketplace option offered to any participants. As an example, 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 [12].

Ashley Madison is the most famous name dating website in infidelity and married dating [12]. Kim Zetter (2015) claim that the data released by the hackers includes names, passwords, addresses and phone numbers submitted by users of the site. On top of that, an analysis of email addresses found in the data dump also shows that some 15,000 are .mil. or .gov addresses indicating that some users were parts of the US government and that their credentials might have been affected [12]. Moreover, in 2013, the Australian Police Department has confirmed that the hackers so-called "Medicare Machine" offered private Medicare details to anyone requesting them, all for a fee of 0.0089 bitcoin -- equivalent to AU$30.50 on the Dark Web [13]. In 2017, Target was hacked and customers card detailed turned up for sales of the Dark web [14].

Another famous example of a dark network was the Silk Road marketplace founded in 2011 and often considered the first dark net market [15].These kind of marketplace were instrumental in the development of cryptocurrencies such as Bitcoin, which rely on decentralization and enhanced security measures. Even though it was busted in 2013 by government authorities, many copycat market were reproduced after [16]. This shows us how dangerous these online black markets are for people nowadays. Practically anything one need to know or have access to is available on the Dark web.

As a result, on these secret websites existing on encrypted network, individuals hosts websites that not every common internet user can have access. While many of these websites are host on the dark for illegal purposes, they can be used to protect individual from surveillance, facilitate news leaks and used to protect political from reprisal [17]. So, aside from illegal activity perpetrated on the Darknet, there are legitimate reasons one might use this kind of market.

Figure 1: Sample of Darknet Website [17]

4.1 ACCESSING THE DARKNET

Furthermore, to access Dark Web or Black Market's websites, you need an anonymizing browser. "Tor" is an example of an open source browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable and untraceable [18]. Tor stands for "the onion routing project" and was developed by the U.S. Navy for the government in the mid-1990s. The browser is available for any Linux, Mac and Windows system and is now render available on cellphone. Any time you visit a website using a typical browser, you can be traced back to your exact location because your IP address is made unhidden to everyone connected on the website.

On the other hand, Tor allows individuals to hide their location, appearing as if they are in a different country. Tor is a network made up of many of volunteer nodes which are called relays. A relay is a computer inside Tor, listed in the main directory, receiving internet signals from another relay and passes that signal on to the next relay in the path. Consider someone in Jamaica who wants to search a site hosted in Minnesota. Instead of him connecting directly, the Tor browser takes him on at least three random detours called relays. His request may go from Jamaica to South Africa, from South Africa to Hong Kong and from Hong Kong to Minnesota [19]. Using Tor browser make it difficult or impossible for any snoops to see your search history, social or any other online activity because bouncing people request around to random computers all over the world makes it harder for the government to find you [20].

Figure 2: The Tor Network [19]

Furthermore, Tor only works for TCP streams and can be used by any application with SOCKS support [21]. Thus, a path is randomly generated for each connection request and on top of that none of the relays keep records of these connections. Using Tor, you can prevent the sites you visit to have access to your physical location and keep websites to track your history [22]. Seeing how Tor is powerful show us why it is the most preferred ways to host Black market on the websites and why cybercriminal are difficult to get caught by the government.

4.2 DARK WEBSITES

On the same nutshell, 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. Finding a criminal market place is very simple once someone has gotten in the dark web searching for them. As an example, Nucleus was a very popular marketplace on the Darknet that focused primarily in dealing drugs or contraband. But in the late 2016, the website became unresponsive [23]. The marketplace best known for trafficking in identity theft using Tor was Alphabay Market [24]. There are thousands more dark websites that are available on the Black market and many more dark websites are created every rendering criminal investigation more difficult since it is not easy to pinpoint exactly their locations.

5. CYBERCRIME IN THE DARK WEB

The virtual crime is not different from the real-world crime, the virtual crime only employs a new medium of conducting the crime. Virtual crimes are also committed using the computer and the Internet.

- Drug, Weapons and Exotic Animal

Silk Road website is an anonymous marketplace that involves in the selling of cloths, books and illegal goods such as weapons & drugs. On the Tor network, these website appears like every other shopping website on the internet that includes a brief description of the goods and also corresponding photographs [25].

- Stolen Good and Information

The dark web encourages their user to trade sensitive information such as username and password, credit card details, PayPal password etc. [26].

- Murder

Assassination website on the dark web allow its users to predict the date of death of a particular individual and gets a reward when the date of death is guessed accurately. The dark web also include website to hire assassin such as White Wolves [27].

- Terrorism

Terrorist make use of the dark web because of the anonymous network that is inaccessible. The terrorist cannot use the surface web because their site can be easily shut down and the administrator can be traced. They make use of the dark web for their propaganda, recruitment, planning etc. [28].

- Illegal Financial Transaction

Untraceable financial transaction are conducted by some website in the dark web such as Banker & Co and Instacard. They carry out their activity by issuing a bank anonymous debit card to user or virtual credit card which is used by the dark web trusted operators [29].

- The Hidden Wiki

The hidden wiki is the main inventory used in the dark web. This website encourages cyber-attack, money laundering, contract killing etc. Just like other website on the dark web, the link to the hidden wiki is changed frequently to avoid detection [30].

6. MONITORING OF THE DARK WEB

As earlier mentioned, the Dark web and the Tor network protects cybercriminals presence on the internet and promotes various illegal activities. Security agencies are making effort to track and monitor activities conducted in the dark web by focusing on the Tor network but due to the dark web network design, monitoring of activities has been a huge challenge to the security agencies [31]. The following areas below can be concentrated on to address the challenges:

- Monitoring of Customer Data

Security agencies can monitor and analysis customer web data to identify interaction with the non-standard domain. Thus, this monitoring might not detect links to dark web but it will give the agency an insight on their activities. User privacy would not be comprised during the monitoring, as agencies are interested in the web request destination not the individual accessing the website [32].

- Social Site Monitoring

New hidden service and information are transmitted through a website called “Pastebin”. Under constant monitoring of this site, message exchange that includes new dark web domain can be detected [33].

- Hidden Service Monitoring

Most dark web services are frequently shutdown and relaunched under a new domain after a certain time. Hidden service activity can be monitored by identifying new sites as soon as they are launched and take snapshot in order to be used for future analysis [34] [35] [36].

- Semantic Analysis

After retrieving the hidden services data on the dark web, a semantic database containing importance information about the hidden service can be created. With this database, future illegal activities on the site can be tracked [36].

7. CONCLUSION

The rapid growth of dark web has led to the easy distribution of encrypted technologies and hacking codes making it harder for the cybersecurity domain. Nowadays, we observe a rise in the number of cybercriminals carrying out their activities on the dark web to avoid being tracked by the government. In the wake of highly-publicized arrests and an increase in the ability of law enforcement to take down some markets, criminals are now aware of the risks using the web. As a result, it is necessary for every organization to at least update its security systems to the current standards and always pay attention to network traffic that is flowing through its connections.

References

[1] Kucuk, S. Umit, and Sandeep Krishnamurthy. "An analysis of consumer power on the Internet." Technovation 27, no. 1-2 (2007): 47-56.

[2] Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL Based Medical Data Processing and Retrieval: The Exposome Project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. ACM, 2017.

[3] Goutam, Rajesh Kumar. "Importance of cyber security." International Journal of Computer Applications 111, no. 7 (2015).

[4] Mailewa, Akalanka, Jayantha Herath, and Susantha Herath. "A Survey of Effective and Efficient Software Testing." In The Midwest Instruction and Computing Symposium. Retrieved from http://www.micsymposium.org/mics2015/ ProceedingsMICS_2015/Mailewa_2D1_41. pdf. 2015.

[5] Reddy, G. Nikhita, and G. J. Reddy. "A Study of Cyber Security Challenges and its emerging trends on latest technologies." arXiv preprint arXiv:1402.1842 (2014).

[6] Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. "A Review of MongoDB and Singularity Container Security in regards to HIPAA Regulations." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91-97. ACM, 2017.

[7] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs." In Companion Conference of the Supercomputing-2018 (SC18), 2018.

[8] Hardy, Robert Augustus, and Julia R. Norgaard. "Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web." Journal of Institutional Economics 12, no. 3 (2016): 515-539.

[9] Beckert, Jens, and Frank Wehinger. "In the shadow: illegal markets and economic sociology." Socio-Economic Review 11, no. 1 (2012): 5-30.

[10] Nardo, Massimo. "Economic crime and illegal markets integration: a platform for analysis." Journal of Financial Crime 18, no. 1 (2011): 47-62.

[11] Buxton, Julia, and Tim Bingham. "The rise and challenge of dark net drug markets." Policy brief 7 (2015): 1-24.

[12] Zetter, Kim. "Hackers Finally Post Stolen Ashley Madison Data." Wired. June 29, 2017. Accessed March 22, 2019. https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

[13] Reilly, Claire. "Inside the Dark Web: A Guide to the Badlands of the Internet." CNET. November 30, 2017. Accessed March 22, 2019. https://www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/.

[14] Reilly, Claire. "Inside the Dark Web: A Guide to the Badlands of the Internet." CNET. November 30, 2017. Accessed March 22, 2019. https://www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/.

[15] Van Hout, Marie Claire, and Tim Bingham. "'Silk Road', the virtual drug marketplace: A single case study of user experiences." International Journal of Drug Policy 24, no. 5 (2013): 385-391.

[16] Roderic, B., G. Peter, A. Mamoun, and C. Steve. "Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime." International Journal of Cyber Criminology 8, no. 1 (2014): 1-20.

[17] "Krebs on Security." Brian Krebs. Accessed March 22, 2019. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[18] Chertoff, Michael. "A public policy perspective of the Dark Web." Journal of Cyber Policy 2, no. 1 (2017): 26-38.

[19] Guccione, Darren, Darren Guccione, and IDG Contributor Network. "What Is the Dark Web? How to Access It and What You'll Find." CSO Online. January 11, 2019. Accessed March 22, 2019. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

[20] Jardine, Eric. "Tor, what is it good for? Political repression and the use of online anonymity-granting technologies." New media & society 20, no. 2 (2018): 435-452.

[21] Mohajeri Moghaddam, Hooman, Baiyu Li, Mohammad Derakhshani, and Ian Goldberg. "Skypemorph: Protocol obfuscation for tor bridges." In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 97-108. ACM, 2012.

[22] Weinberg, Zachary, Jeffrey Wang, Vinod Yegneswaran, Linda Briesemeister, Steven Cheung, Frank Wang, and Dan Boneh. "StegoTorus: a camouflage proxy for the Tor anonymity system." In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 109-120. ACM, 2012.

[23] Paquet-Clouston, Masarah, and Judith Aldridge. "Conflict Managem ent in IllicitReprints and permission." International Criminal Justice Review 27, no. 4 (2017): 237-254.

[24] Celestini, Alessandro, Gianluigi Me, and Mara Mignone. "Tor marketplaces exploratory data analysis: the drugs case." In International Conference on Global Security, Safety, and Sustainability, pp. 218-229. Springer, Cham, 2017.

[25] Chertoff, Michael, and Tobby Simon. "The impact of the dark web on internet governance and cyber security." (2015).

[26] Kim, Won, Ok-Ran Jeong, Chulyun Kim, and Jungmin So. "The dark side of the Internet: Attacks, costs and responses." Information systems 36, no. 3 (2011): 675-705.

[27] Weimann, Gabriel. "Lone wolves in cyberspace." Journal of Terrorism Research (2012).

[28] Weimann, Gabriel. "Going dark: Terrorism on the dark web." Studies in Conflict & Terrorism 39, no. 3 (2016): 195-206.

[29] Piazza, Fiammetta. "Bitcoin in the dark web: a shadow over banking secrecy and a call for global response." S. Cal. Interdisc. LJ 26 (2016): 521.

[30] Bénel, Aurélien, Chao Zhou, and Jean-Pierre Cahier. "Beyond Web 2.0… And Beyond the Semantic Web." In From CSCW to Web 2.0: European Developments in Collaborative Design, pp. 155-171. Springer, London, 2010.

[31] McCoy, Damon, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. "Shining light in dark places: Understanding the Tor network." In International symposium on privacy enhancing technologies symposium, pp. 63-76. Springer, Berlin, Heidelberg, 2008.

[32] Oprea, Alina M., Zhou Li, Robin Norris, and Kevin D. Bowers. "Detection of malicious web activity in enterprise computer networks." U.S. Patent 9,838,407, issued December 5, 2017.

[33] Hassan, Nihad A., and Rami Hijazi. "Social Media Intelligence." In Open Source Intelligence Methods and Tools, pp. 203-260. Apress, Berkeley, CA, 2018.

[34] Mokaddem, Sami, Gérard Wagener, and Alexandre Dulaunoy. "AIL-The design and implementation of an Analysis Information Leak framework." In 2018 IEEE International Conference on Big Data (Big Data), pp. 5049-5057. IEEE, 2018.

[35] Sood, Aditya K., Sherali Zeadally, and Rohit Bansal. "Cybercrime at a scale: A practical study of deployments of HTTP-based botnet command and control panels." IEEE Communications Magazine 55, no. 7 (2017): 22-28.

[36] Mailewa, Akalanka, and Jayantha Herath. "Operating Systems Learning Environment with VMware." In The Midwest Instruction and Computing Symposium. Retrieved from http://www.micsymposium.org/mics2014/ ProceedingsMICS_2014/mics2014_submission_14.pdf. 2014.

[37] Romeo, A. Dominick. "Hidden threat: the dark web surrounding cyber security." N. Ky. L. Rev. 43 (2016): 73.