https://kiisc.or.kr

2022년 한국정보보호학회 동계학술대회

CISC-W'22

Conference on Information Security and Cryptography-Winter 2022

2022년 11월 26일 (토) | 국민대학교

- 학술대회 등록대: 미래관 자율주행 스튜디오 (4층)
- 개회식/정기총회: 본부관 (1층)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KMU 국민대학교 KOOKMIN UNIVERSITY

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 지란지교시큐리티, PILAB

한국정보보호학회
Korea Institute of Information Security & Cryptology

일상활동이론에 연계한 다크웹 대상 분석적 인스펙션에 관한 연구

서영일* , 박기웅†

세종대학교 시스템보안연구실 (지능형드론 융합전공)

세종대학교 정보보호학과

Analytic Inspection on the Dark Web with Routine Activity Theory

Youngil Seo* , Ki-Woong Park†

SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University

† Department of Computer and Information Security, Sejong University

Abstract

The dark web is a segment of the deep web on the Internet that can only be accessed with specialized software, such as a reliable VPN and Tor browser. The dark web contains cybercriminal activities, such as malware software, terrorist attacks, drugs, and black markets. The evolution of the dark web among hackers and cybercriminal groups is an increasing concern on the Internet of the digital world. This study aims to focus on how the dark web can be used to collect essential information for investigating crimes as an information-gathering tool and provide an analysis of how illegal activity on the dark web is evolving using a systematic analysis with the routine activity theory. The results from this study provide a comprehensive view of patterns of criminal activity.

I. Introduction

The power of the Internet has made it possible for people to communicate whenever they want over the World Wide Web platform. This has increased online communication over the Internet. Individuals on the Internet use regular search engines, such as Google, to search for information. However, there are secret services hidden from those search engines. These services are known as the dark web, leading to the absence of darknets and the anonymous Tor browser.

The dark web is also recognized as darknets or dark web. It is a part of the deep web that users cannot look into without restricted software applications [1]. This signifies that anyone can get into it if individuals have installed the required software. The dark web provides encryption services to hide the identity of each user; therefore, individuals can be anonymous in the context of their IP address. Unlike other websites, the dark web is the place where illegal goods and information are purchased and sold. Hence, it is risky because other people can use it for evil and wicked purposes. Also, people can get malware infections or ransomware attacks on their computers by clicking or downloading something without knowing the product on the dark web.

This survey aims to investigate the analysis of the methodology for inquiring crimes on the dark web as an information-gathering tool and provide

† Corresponding author: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 2020년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(UD210029TB)의 지원을 받아 수행되었습니다.

an analysis of the criminal activity patterns of the dark web based on Cohen and Felson's routine activity theory to interpret and understand the motivational factors from criminals.

The remainder of this paper is structured as follows: Section II provides the background information of this topic. Section III describes research method strategy for gathering the most relevant research studies related to the topic. Section IV describes the dark web as an information-gathering tool to provide the analytical methodology investigation. Section V describes the pattern of criminal activity using the routine activity theory. Finally, section VI concludes the paper.

I. Background

The power of anonymity on the dark web is the primary source for hackers and cybercriminal groups to share illegal goods, upload ransomware, sell malware applications, and create private communication channels with other criminal groups. The contents of the dark web use anonymous network services using the TOR software browser, which provides confidentiality and integrity services with Internet privacy. The design of the onion networks on the dark web makes cybercriminal groups to create criminal activities. This is one of the main reasons that hackers and criminal groups commit criminal activities.

Routine activity theory gives a systematic analysis to identify, evaluate, and interpret criminal situations and motivational factors, such as how hackers and criminal groups commit particular crimes. Marcus Felson and Lawrence E. Cohen proposed the routine activity theory and suggested that any crime can happen with three elements. These elements are the motivated attackers, appropriate targets, and the absence of skilled defenders [2]. Crimes are frequently occurred with these factors, leading to the evolution of illegal activities.

Figure 1 illustrates the concept of routine activity theory and how criminal activity is related to three elements.

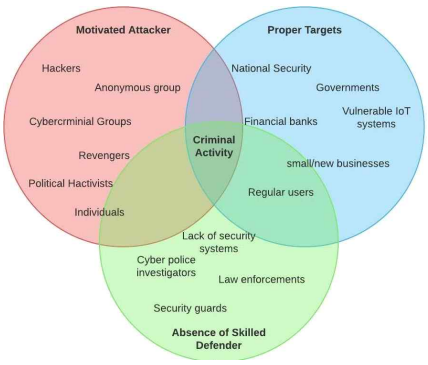

Fig.1 Routine Activity Theory

Digital space has also a similar environment with the actual world that online users create illegal subcultures within the virtual community [2]. There are many criminal motivations for committing crimes on the dark web. Hackers and cybercriminal groups who commit financial crimes are motivated by money. Criminal groups who commit political crimes or propaganda are motivated by their harmful objectives. Other criminal groups, such as the anonymous group, who commit ransomware attacks are inspired by money or taking an act of revenge on someone. This result is how illegal activity on the dark web is evolving, changing, cycling and returning to a functional form.

II. Research Method Strategy

After finding recent research studies, what it calls into question was pinpointing and structuring the most relevant research studies considering the topic. The research solution strategy taken for this search was finding a critical keyword search using a search engine to find and retrieve relevant articles and publications [3]. The primary source used for this search was Google Scholar. By searching, typing, and using keywords, such as "dark web," "threats," and "anonymous", the search engine provided articles related to those particular words. However, there is a restricted line of getting certain information about the dark web or dark net academically due to the unindexed contents of the dark web topic [3].

III. Dark web as an Information gathering tool

The dark web is a specific website for getting certain information and products, such as drugs, guns, malware services, crimes, and passports. Therefore, it is used as an information-gathering tool to collect various information. Compared to regular websites, security professionals often use the dark web to analyze digital evidence, investigate crimes, and catch cybercriminal groups.

The dark web is used as a tool to collect vital information with the analytical methodology for investigating crimes on the dark web. The analytical method of investigation for inquiring crimes is primarily data web mining techniques using the power of machine learning. In this data mining methodology, the preliminary information must transmit to the crawling system, and retrieve the data to analyze through data web mining techniques. The web mining techniques can be classified into three procedures [4]. The first step is web data extraction, which extracts the information from the web, analyzes the data, and outputs it into a structured format. The second step is the data pre-processing. This step changes data into a specific form by eliminating the size of the data. The last step in a web data mining technique is the process of mining to extract data patterns using machine learning technology. Consequently, it can find the most relevant crimes on the dark web corresponding to the extracted information as an information-gathering tool. Figure 2 shows how web crawlers work on the dark web:

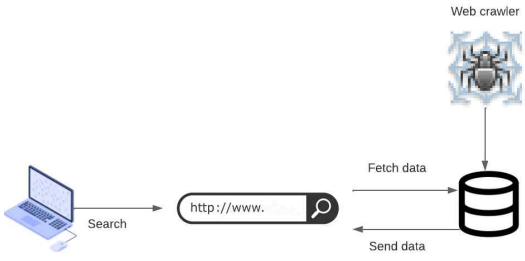

Fig.2 Crawling diagram

IV. Analysis with Routine Activity Theory

Routine activity theory is a theory that explains criminal situations and motivational factors or purposes why criminal groups commit specific crimes. This theory shows the connection between criminals and illegal activity, which explains and analyzes the pattern of criminal activity on the dark web. According to this theory, the pattern of criminal activity can occur depending on the attacker, targets, and absence of defenders. For example, hacktivist groups might use the dark web to attack the government with propaganda to accomplish their political goals. This example demonstrates three elements mentioned in the routine activity theory. First, according to the example, hacktivist groups are motivated attackers who decide to attack the government as their target and achieve their goals with political propaganda, as there is no protector for this political power.

When criminal groups, such as the anonymous group, perform criminal activity on the dark web, attackers make a dedicated plan to attract their targets preferred by the target to attack something or someone. For instance: Revengers might use the dark web to buy ransomware to attack companies for firing. Referring to the routine activity theory, the target attractiveness of criminal activity on the dark web is accessibility. To attack specific organizations from the attacker's perspective, motivated attackers access the dark web where they can easily buy ransomware programs and remain anonymous, engaging in criminal activity with particular motivations. This example demonstrates why the criminal activity is occurring. As a result, the pattern of criminal activity on the dark web is cycling and returning to a functional form even if security professionals keep monitoring the dark web.

Figure 3 shows how the three components in the routine activity theory are correlated with criminal activities on the dark web.

V.Conclusion

In this paper, we review an overview of the

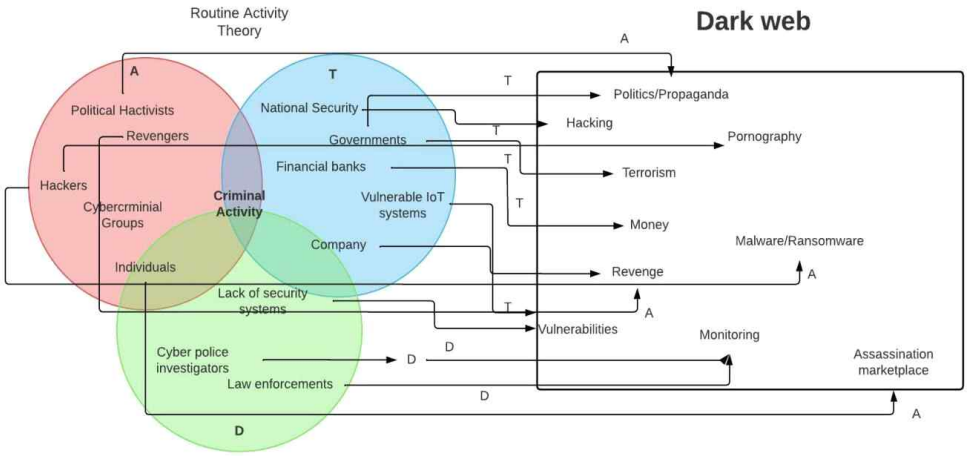

Fig.3 Correlation diagram

dark web, focusing on the analysis of the methodology for inquiring crimes on the dark web as an information-gathering tool and how the pattern of illegal activity on the dark web is evolving and cycling using the theoretical analysis of routine activity theory. Consequently, the existence of the dark web is uncertain as domain URL links keep updating [5], and it is dangerous for people who trade illegal goods. However, this debate may be completed as new technology emerges and moves to the point where Internet privacy is optional to remain anonymous in the future.

[References]

[1] J. Saleem, R. Islam and M. A. Kabir, "The Anonymity of the Dark Web: A Survey," in IEEE Access, vol. 10, pp. 33628-33660, 2022, doi: 10.1109/ACCESS.2022.3161547.

[2] Jung, B. R., Choi, K. S., & Lee, C. S. (2022). Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. International Journal of Cybersecurity Intelligence & Cybercrime, 5(2), 2.

[3] Gupta, A., Maynard, S. B., & Ahmad, A. (2021). The dark web phenomenon: A review and research agenda. arXiv preprint arXiv:2104.07138.

[4] Alshammery, M. K., & Aljuboori, A. F. (2022). Crawling and Mining the Dark Web: A Survey on Existing and New Approaches. Iraqi Journal of Science, 1339-1348.

[5] Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: A systematic approach. IEEE Access, 8, 171796-171819.