International Journal of Cybersecurity Intelligence & Cybercrime

Volume 5 | Issue 2 Article 1

8-22-2022

Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation

cybercrime; darknet market; cryptocurrency; kerberoasting; cyberattack

Recommended Citation

Recommended Citation Choi, S. & Parti, K. (2022). Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation. International Journal of Cybersecurity Intelligence & Cybercrime: 5(2), 1-3. Available at: https://doi.org/10.52306/JQPO4457 Copyright © 2022 Sinyong Choi and Katalin Parti

IJCIC Center for Cybercrime Investigation & Cybersecurity

Choi & Parti (2022). *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(2), 1-3.

Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation

Sinyong Choi, Ph.D., Kennesaw State University, U.S.A.
Katalin Parti*, Ph.D., Virginia Tech, U.S.A.

Keywords: Cybercrime; Darknet market; Cryptocurrency; Kerberoasting; Cyberattack

Abstract:
Cryptography has been applied to a range of modern technologies which criminals also exploit to gain criminal rewards while hiding their identity. Although understanding of cybercrime involving this technique is necessary in devising effective preventive measures, little has been done to examine this area. Therefore, this paper provides an overview of the two articles, featured in the special issue of the *International Journal of Cybersecurity Intelligence and Cybercrime*, that will enhance our understanding of cryptography-related crime, ranging from cryptocurrency and darknet market to password-cracking. The articles were presented by the winners of the student paper competition at the 2022 International White Hat Conference.

Introduction

Cryptography is a method of converting plaintexts into ciphertexts, and vice versa. It is widely used in everyday life to store and transmit data confidentially and securely while protecting its integrity, such as computer passwords, e-commerce transactions, and cryptocurrency. However, criminals also find various criminal opportunities revolving around this technique either by exploiting its anonymous nature to hide their identity while conducing illicit trades using cryptocurrency on darknet markets or by attacking its authentication protocols to steal data (Choi et al., 2022). Although there is an increasing demand to counter the evolving contemporary threats from these cybercrimes, it is known that many law enforcement agencies have suffered from a lack of capabilities for a successful investigation and prosecution of these ever-evolving cybercriminals (Choi, 2015). As an effort to meet this challenge, the third International White Hat Conference was held in 2022, focusing on the "Evolution of Illicit Crypto Use: Current Approaches and Future Challenges for Financial and Government Sectors." The conference hosted a student paper competition in which participants addressed current criminal issues revolving around cryptography. Following is a brief overview of the two winning participants' research.

Jung et al. (2022) collected data from Dark Web financial websites to explore (1) what main products scammers encourage customers to purchase, (2) how financial market vendors operate their business, and (3) which marketing strategies are used to scam potential buyers in the dark web financial market. In recent years, Dark Web financial marketplaces have grown exponentially, providing a platform for traders to exchange illegal goods and services anonymously. Through the sale of hacked credit cards to stolen cryptocurrency accounts, the Dark Web has expanded the scope of illegal activities. This study is designed

*Corresponding author
Katalin Parti*, Ph.D., Department of Sociology, Virginia Tech, 560 McBryde Hall (0137), 225 Stanger St, Blacksburg, Virginia, 24061, U.S.A.
Email: kparti@vt.edu

to identify the characteristics of the Dark Web financial market and its scams. Using Dark Web search engines, data were collected from leading Dark Web financial websites, such as Hidden Wiki, Onion List, and Dark Web Wiki. A thematic content analyses of the content of the Dark Web is combined with statistical analysis. Interpreting the findings through routine activities theory, the author finds that there is potential fraud and scams committed on darknet financial websites, offering important implications for cybercrime investigations. According to the findings, promotions and customer service were provided on Dark Web markets using cryptocurrencies in a similar manner to the Surface Web's e-commerce market. It appears that scams are likely to target buyers in the financial market on the Dark Web. Additionally, dark web sellers construct websites to sell scam products and recommend the purchase of escrow services to ensure safe transactions. The authors conclude that routine activity theory can be used to provide a more comprehensive understanding of the patterns of fraud and scam behavior in the Dark Web financial market. Several effective preventive measures are discussed, including strengthening law enforcement's ability to investigate financial markets as well as promoting public awareness and consumer safety programs. Interpreting the findings through routine activities theory, the authors find that fraud and scams can be potentially committed on darknet financial websites. The paper concludes by offering important implications for cybercrime investigations.

Demers & Lee (2022) describe Kerberoasting which is an active directory-based attack. The reader gets to know that Kerberos is a network authentication protocol used in Windows Active Directory. In the process of authentication, the client connects and interacts with the network authentication service, obtains tickets from the Key Distribution Center (KDC) which may be used in order to communicate with the application servers. Kerberoasting is an attack where an attacker steals the encrypted Kerberos TGS ticket, and then the attacker attempts to crack it offline. Kerberos uses an NTLM Hash in order to encrypt KRB_TGS of the given service. When the domain user sends a request for a TGS ticket to KDC for any service that has a registered SPN, the KDC generates the KRB_TGS without identifying the user authorization against a requested service. The Kerberos protocol uses either symmetric-key or public-key cryptography to provide secure communication with other services and applications on the network. After the literature review, the author provides case study examples, and detailed policy considerations. The manuscript can be useful for practitioners in the fields of cybersecurity and investigation.

Concluding Remarks

It is our responsibility as criminologists to tackle a criminal justice issue and provide a better understanding of it to actors in the criminal justice system; especially the issue which professional and technical knowledge is required to properly understand. In this sense, the articles featured in this special issue are impressive in addressing cybercrime involving complex technologies in a way to be easily understood by readers. We believe the findings and preventive measures suggested in the research would not only contribute to effective criminal justice policies but also provide insights to future research in the field of cybercrime and cybersecurity.

References

Choi, K. (2015). *Cybercriminology and digital investigation*. LFB Scholarly Publishing.
Choi, K., Back, S., & Toro-Alvarez, M.M. (2022). *Digital Forensics & Cyber Investigation*. Cognella.

Demers, D., & Lee, H. (2022). Kerberoasting: Case studies of an attack on a cryptographic authentification techonlogy. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*(2), 25-39.

Jung, B., R., Choi, K., & Lee, C. S. (2022). Dynamics of dark web financial marketplace: An exploratory study of underground fraud and scam business. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*(2), 4-24.