Apr 20th, 12:00 AM - 12:00 AM

Assessing the Frequency and Severity of Malware Attacks: An Exploratory Analysis of the Advisen Cyber Loss Dataset

Ahmed M. Abdelmagid
Old Dominion University

Farshid Javadnejad
Old Dominion University

C. Ariel Pinto
Old Dominion University

Michael K. McShane
Old Dominion University

Rafael Diaz
Virginia Modeling, Analysis, and Simulation Center, Old Dominion University

See next page for additional authors

Author/s
Ahmed M. Abdelmagid, Farshid Javadnejad, C. Ariel Pinto, Michael K. McShane, Rafael Diaz, and Elijah Gartell

ASSESSING THE FREQUENCY AND SEVERITY OF MALWARE ATTACKS: AN EXPLORATORY ANALYSIS OF THE ADVISEN CYBER LOSS DATASET

Abdelmagid, A. M[1,2], Javadnejad, F[1], Pinto, C. A[1], McShane, M[2], Diaz, R[3], and Gartell, E[4]

[1] Engineering Management & Systems Engineering, Old Dominion University, VA 23529
[2] Production Engineering Department, Alexandria University, Alexandria 21544, Egypt
[3] Department of Finance, Old Dominion University, Norfolk, VA 23529
[4] Virginia Modeling, Analysis & Simulation Center, Old Dominion University, Norfolk, VA 23529
[5] School of Cybersecurity, Old Dominion University, Norfolk, VA 23529
aabde005@odu.edu, fjava001@odu.edu, cpinto@odu.edu, mmcshane@odu.edu, rdiaz@odu.edu, egart002@odu.edu

ABSTRACT

In today's business landscape, cyberattacks present a significant threat that can lead to severe financial losses and damage to a company's reputation. To mitigate this risk, it is essential for stakeholders to have an understanding of the latest types and patterns of cyberattacks. The primary objective of this research is to provide this knowledge by utilizing the Advisen cyber loss dataset, which comprises over 137,000 cyber incidents that occurred across various industry sectors from 2013 to 2020. By using text mining techniques, this paper will conduct an exploratory data analysis to identify the most common types of malware, including ransomware. Furthermore, the study will include a likelihood and severity analysis to evaluate the financial impact of these cyberattacks on businesses. Ultimately, this study aims to shed light on the prevalence and financial repercussions of malware incidents and provide businesses with valuable insights to help develop effective cybersecurity strategies.

Keywords: Ransomware, Malware, Cyber-attack, Advisen data loss, Likelihood, Severity

INTRODUCTION

The widespread use of electronic devices and internet-based systems has increased cyber risk for businesses due to exploitation of vulnerabilities in cyber networks to carry out cybercrimes. This paper aims to conduct exploratory data analysis on the Advisen dataset, which contains over 137K cyber incidents that occurred between 2013 and 2020 across various industry sectors. Utilizing text mining, the study aims to identify the most frequently reported malware/ransomware types and propose a likelihood and severity analysis to measure the financial consequences of each type. The insights gained from this analysis could help organizations better understand the nature and impact of cyber threats and develop more effective cybersecurity strategies.

PROPOSED METHODOLOGY

To identify the primary types of malware (including ransomware) from the Advisen data loss, we utilized a systematic approach (Figure 1). After examining the "Case description" column and filtering the data with specific keywords, we verified and analyzed the identified names using a text mining algorithm developed with Python 3.9. Additionally, we searched for well-known malware and ransomware names on various online platforms such as internet databases, research articles, blogs, and technical and organizational websites.. We determined the frequency of occurrences for each identified malware/ransomware and performed a severity analysis to evaluate the average total financial losses incurred by companies due to these incidents.

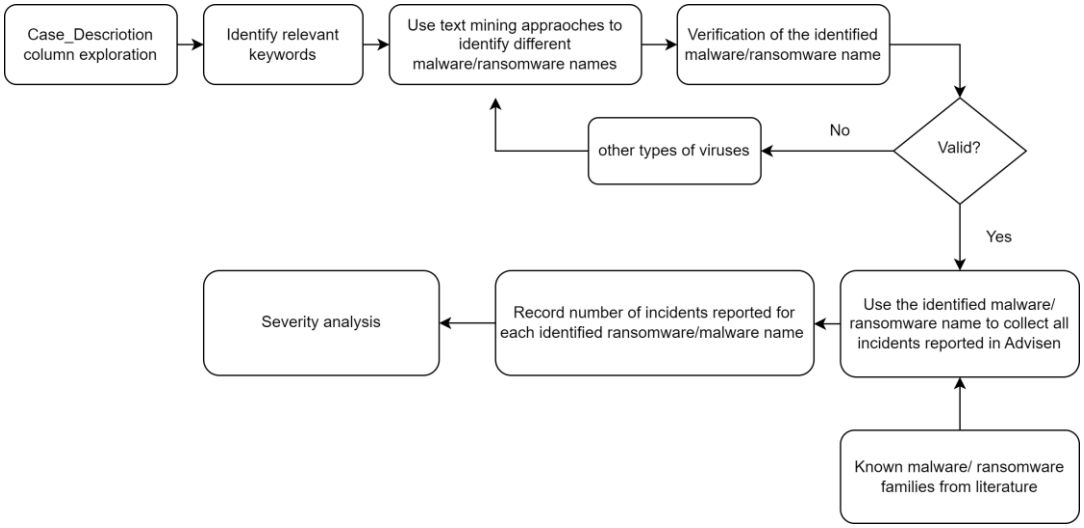

Figure 1: Flowchart of the procedure followed.

EXPECTED RESULTS

The paper analyzes ransomware/malware attacks, emphasizing the need for organizations to be proactive in cybersecurity efforts. Analyzing attack frequency and financial impact helps identify significant threats and safeguard systems and data. Even low-frequency attacks can result to significant losses, hence having robust cybersecurity measures is crucial. The findings suggest attackers target both large and small organizations. Overall, the paper provides valuable insights into the evolving cyber threat landscape, highlighting the need for organizations to stay vigilant in their cybersecurity efforts.

REFERENCES

Abdelnabi, A. A., Abdelmagid, A. M., Rabadi, G., Sousa-Poza, A., & Pinto, C. A. (2022). Risk-and-Resiliency-Intelligent Supply Chain (RRiSC).

Basiri, M. H., Javadnejad, F., & Saeidi, A. (2015). Forecasting crude oil price with an artificial neural network model based on a regular pattern for selecting of the training and testing sets using dynamic command-line functions. 24th International Mining Congress & Exhibition of Turkey (IMCET), Antalya, Turkey

Cheung, K.-F., & Bell, M. G. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research, 291(2), 471-481.

Ghavidel, A., Ghousi, R., & Atashi, A. (2022). An ensemble data mining approach to discover medical patterns and provide a system to predict the mortality in the ICU of cardiac surgery based on stacking machine learning method. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 1-11.

Javadnejad, F., Sharifi, M. R., Basiri, M. H., & Ostadi, B. (2022). Optimization Model for Maintenance Planning of Loading Equipment in Open Pit Mines. European Journal of Engineering and Technology Research, 7(5), 94-101.

Pinto, C. A., Keskin, O. F., Kucukkaya, G., Poyraz, O. I., Alfaqiri, A., Tatar, U., & Kucukozyigit, A. C. (2021). Cybersecurity acquisition framework based on risk management: Economics perspective.

Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1), 138-156.

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. Computers & Security, 109, 102385.