Annotated Bibliography: Computer Malware Detection and Prevention

VINEETHA GALI

New England College

Graduate & Prof Skills Development- 202207-CRN140

Dr. Pollak

July 29th, 2022

Annotated Bibliography: Computer Malware Detection and Prevention

Faruk, M. J. H., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., ... & Wu, F. (2021, December). Malware detection and prevention using artificial intelligence techniques. In *2021 IEEE International Conference on Big Data (Big Data)* (pp. 5369-5377). IEEE.

Computer malware can be defined as a particular code or file usually delivered on a network. This research explores, infects, steals, or even does any the attacker may want to do on your system. This study focuses on computer malware detection and also various measures that can be used to prevent it. Due to the advancement in technology, security has been one of the major problems since there has been an increase in malicious activity, which poses a severe threat to security and the safety of stakeholders with the computer systems. According to Faruk (2021), data protection from fraudulent activity can be identified as a pressing concern to maintain the stakeholders, specifically the end user's security. In this study, the users who face difficulties differentiating between benign and malicious applications are naïve. In this article, the authors mention that mobile and computer systems must be designed to detect malicious activities, thus protecting stakeholders quickly. Several algorithms can see malicious activities through concepts like Deep learning, Artificial Intelligence, and Machine Learning. This article emphasizes the Artificial Intelligence (AI) based methods used in detecting and preventing malware events. This article reviews the current way of seeing malware, its shortcomings, and various techniques to enhance its efficiency.

Dada, E. G., Bassi, J. S., Hurcha, Y. J., & Alkali, A. H. (2019). Performance evaluation of machine learning algorithms for detection and prevention of malware attacks. *IOSR Journal of Computer Engineering*, *21*(3), 18-27.

This article aims at understanding various malware detection and the methods used to control the malware. According to the authors in this article, malware can be referred to as any computer program that is usually developed to wreak havoc on a network or even a computer system. Some examples of computer malware include worms, viruses, adware, and keylogger. The authors of this article mentions that due to the advancement in technology, there is a higher rate of malware growth which poses a significant threat to the security of confidential data. Low performance is usually the main issue with classification algorithms regarding their capability to detect and prevent malware. According to the authors, evaluating the existing machine learning algorithm's performance is essential. Through this, it can assist in the creation of an efficient algorithm that can be used to detect malware.

Akinde, O. K., Ilori, A. O., Afolayan, A. O., & Adewuyi, O. B. (2021). Review of Computer Malware: Detection and Preventive Strategies. *Int. J. Comput. Sci. Inf. Secure.(IJCSIS), 19*, 49.

Malware is known as the malevolent program, code, or even software. It can generally be identified as the program which is usually introduced in a system in a hidden way, aiming to compromise the integrity, secrecy, or accessibility of a victim's data. This research has the purpose of detecting malware and its preventive measures. This article mentions that malware is usually developed to conduct crimeful or delictuous activities in a system. The study shows that in 2000, malware's inhibition and infestation mainly aimed at denial of service and system attacks. However, currently, several people have been malware and cyberwars. The authors mention that ignorance of this malware has resulted in significant losses among individuals and even corporate organizations. Due to the advancement of technology, there is a clear show that the issues regarding viruses cannot end any time soon. This article also shows the history of the malware, categories, identification methods, and even prevention techniques.