World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:19, No:06, 2025

Comprehensive Review of Adversarial Machine Learning in PDF Malware

Authors : Preston Nabors, Nasseh Tabrizi

Abstract : Portable Document Format (PDF) files have gained significant popularity for sharing and distributing documents due to their universal compatibility. However, the widespread use of PDF files has made them attractive targets for cybercriminals, who exploit vulnerabilities to deliver malware and compromise the security of end-user systems. This paper reviews notable contributions in PDF malware detection, including static, dynamic, signature-based, and hybrid analysis. It presents a comprehensive examination of PDF malware detection techniques, focusing on the emerging threat of adversarial sampling and the need for robust defense mechanisms. The paper highlights the vulnerability of machine learning classifiers to evasion attacks. It explores adversarial sampling techniques in PDF malware detection to produce mimicry and reverse mimicry evasion attacks, which aim to bypass detection systems. Improvements for future research are identified, including accessible methods, applying adversarial sampling techniques to malicious payloads, evaluating other models, evaluating the importance of features to malware, implementing adversarial defense techniques, and conducting comprehensive examination across various scenarios. By addressing these opportunities, researchers can enhance PDF malware detection and develop more resilient defense mechanisms against adversarial attacks.

Keywords : adversarial attacks, adversarial defense, adversarial machine learning, intrusion detection, PDF malware, malware detection, malware detection evasion
Conference Title : ICMLA 2025 : International Conference on Machine Learning and Applications
Conference Location : Copenhagen, Denmark
Conference Dates : June 10-11, 2025