Abstract

Malicious Uniform Resource Locators (URLs) pose a significant cybersecurity threat by carrying out attacks such as phishing and malware propagation. Conventional malicious URL detection methods, relying on blacklists and heuristics, often struggle to identify new and obfuscated malicious URLs. To address this challenge, machine learning and deep learning have been leveraged to enhance detection capabilities, albeit relying heavily on large and frequently updated datasets. Furthermore, the efficacy of these methods is intrinsically tied to the quality of the training data, a requirement that becomes increasingly challenging to fulfill in real-world scenarios due to constraints such as data scarcity, privacy concerns, and the dynamic nature of evolving cyber threats. In this study, we introduce an innovative framework for malicious URL detection based on predefined static feature classification by allocating priority coefficients and feature evaluation methods. Our feature classification encompasses 42 classes, including blacklist, lexical, host-based, and content-based features. To validate our framework, we collected a dataset of 5000 real-world URLs from prominent phishing and malware websites, namely URLhaus and PhishTank. We assessed our framework's performance using three supervised machine learning methods: Support Vector Machine (SVM), Random Forest (RF), and Bayesian Network (BN). The results demonstrate that our framework outperforms these methods, achieving an impressive detection accuracy of 98.95% and a precision value of 98.60%. Furthermore, we conducted a benchmarking analysis against three comprehensive malicious URL detection methods (PDRCNN, the Li method, and URLNet), demonstrating that our proposed framework excels in terms of accuracy and precision. In conclusion, our novel malicious URL detection framework substantially enhances accuracy, significantly bolstering cybersecurity defenses against emerging threats.