Abstract:

Phishing attacks remain one of the most common and destructive cybersecurity threats, exploiting human vulnerabilities to steal sensitive data and credentials. Detecting phishing websites in real-time is crucial for mitigating such attacks. This paper explores an innovative approach to phishing website detection by leveraging Structured Threat Information Expression (STIX) instances and Threat Intelligence Express (TAXII) feeds. STIX provides a standardized format for representing cybersecurity threat intelligence, while TAXII facilitates the automated sharing and consumption of this data between organizations and threat intelligence platforms. By integrating real-time threat intelligence feeds from TAXII into a system that analyzes STIX instances representing known phishing domains, this study demonstrates an efficient method for detecting and responding to phishing websites. The proposed system utilizes pattern matching, reputation scoring, and machine learning models to identify phishing indicators such as suspicious domain names, website characteristics, and behavioral anomalies. This approach significantly improves detection accuracy by incorporating up-to-date threat intelligence, enabling swift mitigation of phishing threats before they can cause significant harm. Results show that the system can identify phishing websites with high precision, offering a proactive solution for enterprises and security teams to combat phishing attacks at an early stage.