FP-TREE AND SVN FOR MALICIOUS WEB CAMPAIGN DETECTION

Kruczkowski, M; Niewiadomska-Szynkiewicz, E; Kozakiewicz, A

Intelligent Information and Database Systems, 7th Asian Conference, ACIIDS 2015; tom 9012; numer ; strony 193-201; 2015; Springer

The classification of the massive amount of malicious software variants into families is a challenging problem faced by the network community. In this paper (The work was supported by the EU FP7 grant No. 608522 (NECOMA) and "Information technologies: Research and their interdisciplinary applications", POKL.04.01.01-00-051/10-00.) we introduce a hybrid technique combining a frequent pattern mining and a classification technique to detect malicious campaigns. A novel approach to prepare malicious datasets containing URLs for training the supervised learning classification method is provided. We have investigated the performance of our system employing frequent pattern tree and Support Vector Machine on the real database consisting of malicious data taken from numerous devices located in many organizations and serviced by CERT Polska. The results of extensive experiments show the effectiveness and efficiency of our approach in detecting malicious web campaigns.

Słowa kluczowe: malware campaign, url
Powrót