Scopus

Documents

Saleh, M.F.

Malware detection model based on classifying system calls and code attributes: A proof of concept
(2019) *International Journal of Electronic Security and Digital Forensics*, 11 (2), pp. 183-193.

Abstract
The process of malware detection involves static code analysis and dynamic analysis. Both methods have limitations. This research tried to bridge the gap between the two methods by dynamically predicting the risk before the static analysis. The proof-of-concept examined the code of known malwares and concluded that five characteristics of the code will predict the risk of any executable file, namely, the system function, encryption, code obfuscation, stalling code, and checking for the debugger environment. The proof-of-concept validates the effectiveness of the model. It shows 96% success and limited false-positives results. Copyright © 2019 Inderscience Enterprises Ltd.

2-s2.0-85063969510
Document Type: Article
Publication Stage: Final
Source: Scopus