Applied Sciences, vol.12, no.3, pp.1076-1-1076-18, .

Evaluation of local security event management system vs. standard antivirus software

A. Pérez Sánchez; R. Palacios Hielscher

Abstract-

The detection and classification of threats in computer systems has been one of the main problems researched in Cybersecurity. As technology evolves, the tactics employed by adversaries have also become more sophisticated to evade detection systems. In consequence, systems that previously detected and classified those threats are now outdated. This paper proposes a detection system based on the analysis of events and matching the risk level with the MITRE ATT&CK matrix and Cyber Kill Chain. Extensive testing of attacks, using nine malware codes and applying three different obfuscation techniques, was performed. Each malicious code was analyzed using the proposed event management system and also executed in a controlled environment to examine if commercial malware detection systems (antivirus) were successful. The results show that evading techniques such as obfuscation and in-memory extraction of malicious payloads, impose unexpected difficulties to standard antivirus software.

Index Terms- SIEM; antivirus; event-based threat detection; MITRE; Cyber Kill Chain

Citation:
Pérez-Sánchez, A.; Palacios, R. "Evaluation of local security event management system vs. standard antivirus software", Applied Sciences, vol.12, no.3, pp.1076-1-1076-18, .