AI-BASED FILE-LESS MALWARE DETECTION ENGINE

Rasindu De Alwis

A dissertation submitted in partial fulfilment of the requirement for
Bachelor of Engineering (Honours) degree in Software Engineering

Department of Computing

Informatics Institute of Technology, Sri Lanka
in collaboration with
University of Westminster, UK

2021

Abstract

The threat footprint has been changed with the evolution of cybersecurity countermeasures over the past few decades, especially in the malware industry from traditional file-based malware to file-less malware. Attackers are making use of the attack techniques that operate directly from the process memory or utilizing pre-installed legitimate tools or services in the system to achieve their goals. Moreover, detection of file-less malware can be tedious, time-consuming, and requires a significant amount of data gathering tasks for any malware analyst as it does not use traditional executables or create new software onto the device to carry out its malicious activities. This makes it far more difficult for traditional signature-based AV and other endpoint security products to detect and prevent because of the low footprint and no files to scan.

In this research, a process model has been documented in order to handle these multifarious file-less malware attacks in the incident response process. So that the proposed system will be able to automate the manual file-less malware investigation workflow to detect file-less attacks at an early stage with fewer false alarms. This will be achieved by chaptering and integrating all possible windows event logs of the suspicious system in real-time. Moreover, these chaptered events will be tagged and classified with a hybrid machine learning algorithm. The proposed hybrid approach is a combination of both supervised and unsupervised algorithms. Each event log is classified with the use of a supervised algorithm and then the classified result will be evaluated with an association analysis algorithm. The process will help to identify the falsely classified results.

Key words:

File-Less Malware, Windows Event Log, Incident Response, Memory Resident Malware, Machine Learning