Early Stage Malware Detection and Threat Prediction Using Machine Learning

KT Dananjana#, PPNV Kumara and WJ Samaraweera

Faculty of Computing, General Sir John Kotelawela Defence University, Sri Lanka
#tharuka.kannangara95@gmail.com

Malware is growing rapidly day by day. Malware creators are creating their malware smarter and smarter. To tackle these problems, security companies are launching different antimalware software and end-point malware analysis software. In Artificial Intelligence, machine Learning is one of the key aspects. Machine Learning algorithms use real-world examples by generalizing to achieve a task. In comparison to procedural programming, machine learning is feasible, efficient, practical and profitable. This paper discusses the meaning of static and dynamic malware analysis and how these concepts are used to tackle our problem. The aim of this study is to investigate how the data collection is done regarding malware and how Microsoft PE header concept is so important in order to achieve the proposed solution regarding malware. This study describes how proposed Machine Learning approach selects the Features, training models and what are the evaluation methods that are going to be used to measure the model accuracies. In conclusion, using the Machine Learning power, it is intended to create a tool in order to detect malware before it infects the computer, and to predict how soon a computer will be hit by a malware or not, as a score in order to save billions worth of data from malware.

Keywords: Malware Detection, Static Malware Analysis, Neural Networks, Machine Learning