Malware detection based on performance counters

Omar Mohamed*
Ciprian-Bogdan Chirila**
*University ..., Turkey
**University Politehnica of Timişoara, Romania
Department of Computers and Information Technology
E-mail: omarmostafa1101@gmail.com; chirila@cs.upt.ro

***Abstract*—**

I. Introduction

In this paper we present a framework for training and evaluating models for detecting malware in operating systems based on performance counters.

... [1] ...

In Figure 1 we present conceptually our approach.

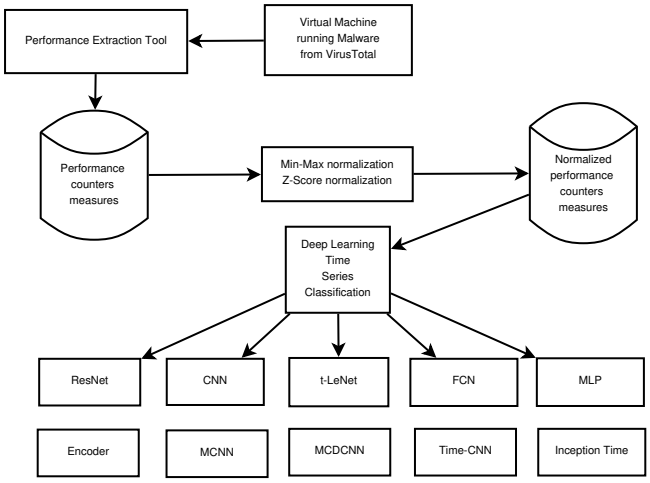

Fig. 1.

We start our approach at a Virtual Machine (VM) running viruses from VirusTotal. On the same VM we run a tool that collects the performance counters into several time series. Next, the results are normalized using statistical operators like Min-Max and Z-Score. On the resulted time series we trained several classification models: i) ResNet; ii) CNN; iii) t-LeNet; iv) FCN; v) MLP; vi) Encoder; vii) MCNN; viii) MCDCNN; ix) Time CNN; x) Inception Time. On the trained classification models accuracy tests were performed and corresponding graphs were plotted.

We consider that the trained classfiers could be used on a real machine as a malware detection tool.

The paper is structured as follows. Section II presents related works in the field of program behaviour analysis and performance counters. Section III presents the design of the performance counters extration tool and the configuration of the classification models. Section IV presents the experimental results from the trained classfication models. Section V analyzes the experimental results. Section VI concludes and sets the future work.

II. Related Works

III. Experimental setup

IV. Experimental results

V. Discussion

VI. Conclusions and Future Work

In this paper we presented an experimental setup where performance counters time series were extracted from a malware infected virtual machine. The performance counter time series were normalized and used to train 10 classification models.

As future work we intend to experiment with the 10 classifiers detecting malware and assessing their performance.

References

[1] Advanced Distributed Learning Initiative. Experience api. http://adlnet.gov/adl-research/performance-tracking-analysis/experience-api/, 2019.