Pune Institute of Computer Technology, PUNE
IT DEPARTMENT
Malware Detection using Deep Learning

Group 21 - Bharat Kothari, Animesh Landge, Shrijan Vats, Amod Dhopavkar

POSTER PRESENTATION

TE PBS GROUP 21

INTRODUCTION

- **With new malwares coming every day, traditional detection techniques do not perform well and there is need for effective zero-day malware detection model**

OBJECTIVES

- **We propose a novel image processing technique with optimal parameters for MLAs and deep learning architectures to arrive at an effective zero-day malware detection model.**
- **We perform a comparative study of our model with other detection models.**

METHODOLOGY

1) **A new proposal of a scalable and hybrid framework which facilitates to collect malware samples from different sources in a distributed way and to apply pre-processing in a distributed manner. The framework has the capability to process large number of malware samples both in real-time and on demand basis.**

2) **A proposal of a novel image processing technique for malware classification.**

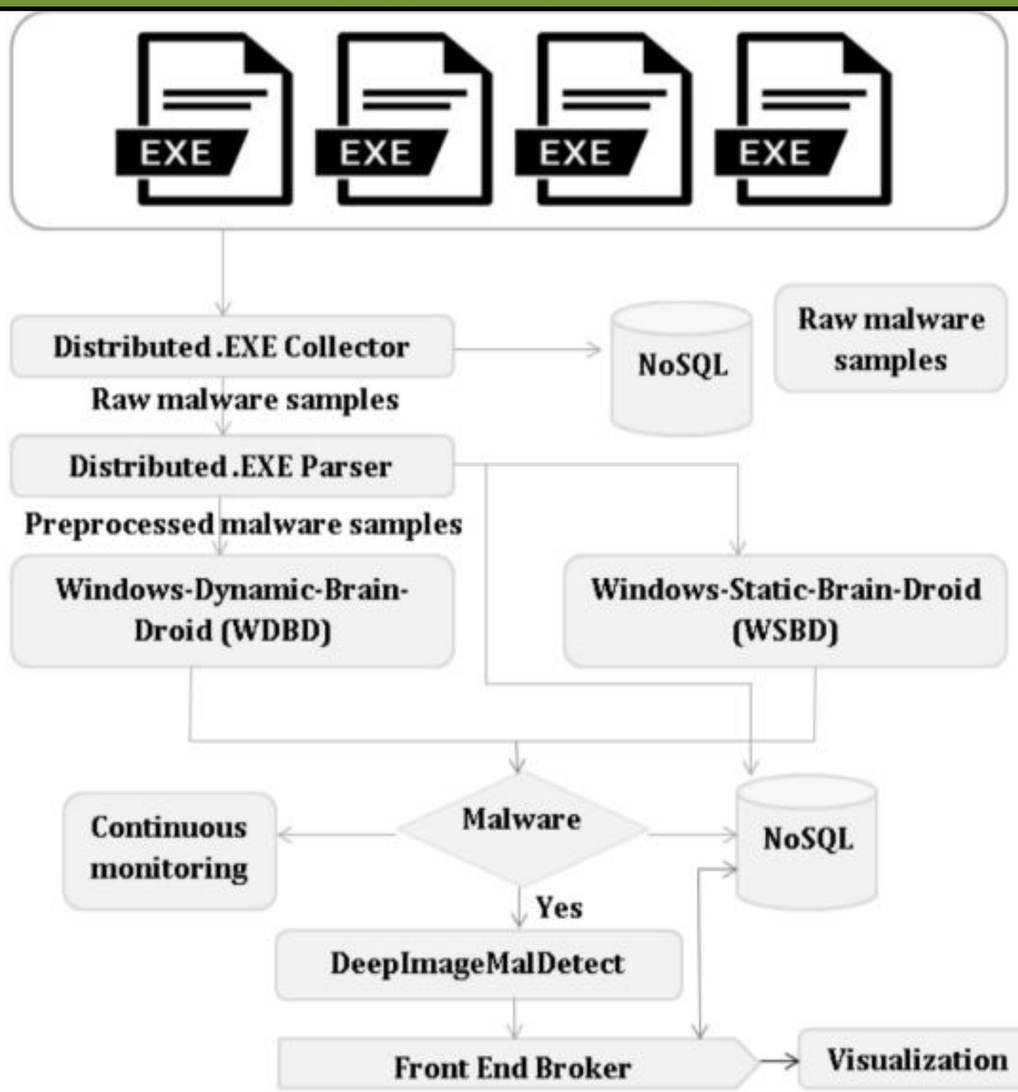
3) **It follows two stage approach, in the first stage the executables file is classified into malware or legitimate using Static and Dynamic analysis and in second stage the malware executables file is categorized into corresponding malware family.**

4) **An independent performance evaluation of classical MLAs and deep learning architectures, benchmarking various malware analysis models.**

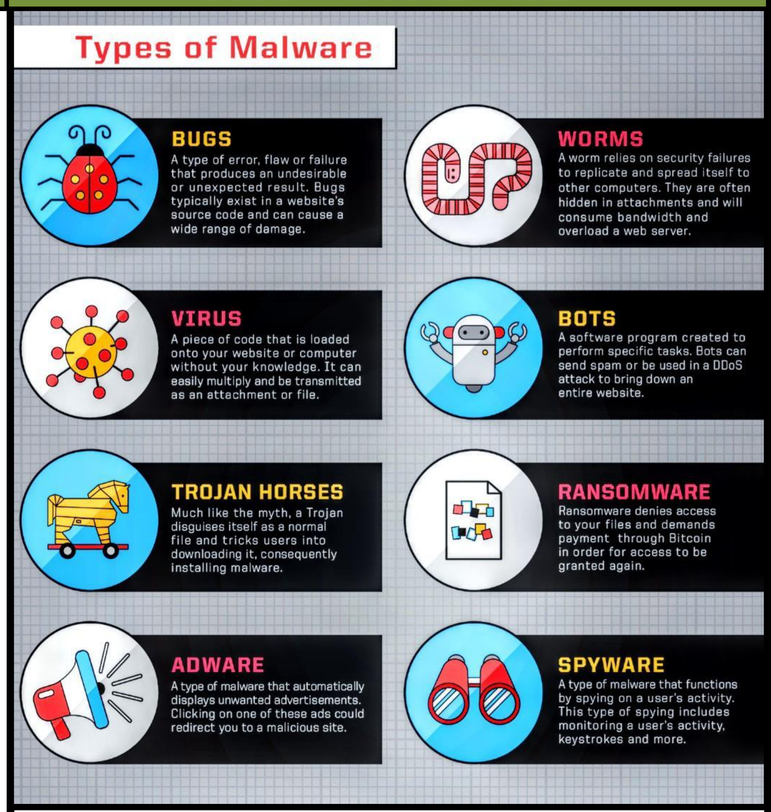
MALWARE DETECTION TECHNIQUES

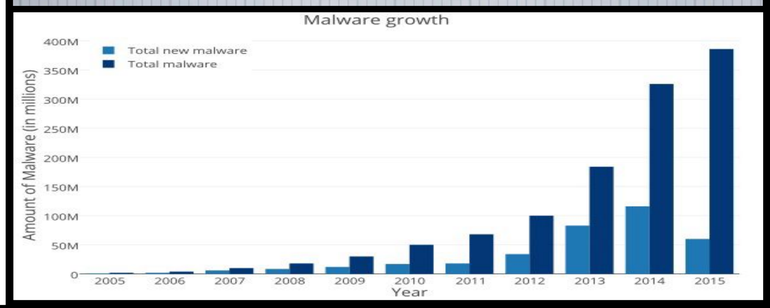
1. **Signature Based Technique :** In this technique, the given malware is searched and matched with existing malwares in a malware definition database table. This technique faces challenges when malware uses code obfuscation.
2. **Static Analysis :** Static analysis is a method that captures the information from the binary program without executing.
3. **Dynamic Analysis :** Dynamic analysis is the process of monitoring malware behavior at run time in an isolated environment. Dynamic analysis can be an efficient long term solution for malware detection system. The Dynamic analysis cannot be deployed in end-point real time malware detection due to the reason that it takes much time to analyze its behavior, during which malicious payload can get delivered.
4. **Machine Learning :** Machine learning algorithms (MLAs) rely on the feature engineering, feature selection and feature representation methods. The set of features with a corresponding class is used to train a model in order to create a separating plane between the benign and malwares. This separating plane helps to detect a malware and categorize it into its corresponding malware family.
5. **Deep Learning :** During the training process, it tries to capture higher level representation of features in deep hidden layers with the ability to learn from mistakes. MLAs experience diminishing outputs as they see more and more data whereas deep learning captures new patterns and establishes associations with the already captured pattern to enhance the performance of tasks.

PROPOSED ARCHITECTURE



TYPES OF MALWARE





CONCLUSIONS

- **We would like to explore this topic further and learn more about how neural networks can be used for detection in malware.**
- **We have read a few papers about malware detection and would like to explore more papers about the same.**
- **We would also like to work on finding ways in which malware can be detected efficiently using the existing methods.**

REFERENCES/PUBLICATIONS

- Robust Intelligent Malware Detection Using Deep Learning - R. VINAYAKUMAR, MAMOUN ALAZAB, (Senior Member, IEEE), K. P. SOMAN, PRABAHARAN POORNACHANDRAN, AND SITALAKSHMI VENKATRAMAN
- https://ieeexplore.ieee.org
- https://dl.acm.org
- https://springer.com/in
- https://sciencedirect.com
- https://researchgate.com