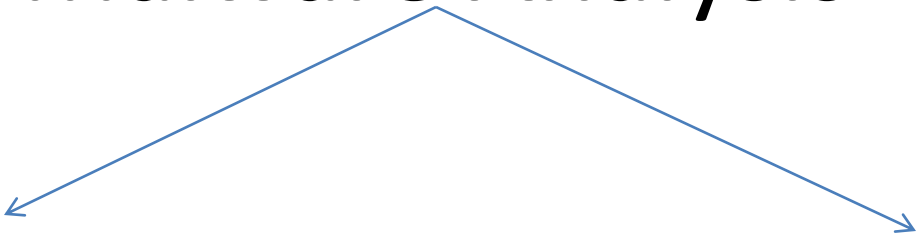
Malware Analysis

Akarsh S

Introduction

- MALWARE: MALicious softWARE, is any software that is designed to cause damage to a computer, server, network, mobile phones and more such devices which poses a serious security threat to financial institutions, businesses and individuals.
- Based on functions malwares are classified into different types such as Trojans , Backdoors , Virus, Worm, Spyware, Adware and more
- There is tremendous increase in the amount of malware being generated today approximately 325000 samples per day
- The main reason for such a deluge is malware mutation: the process of creating new malware variants from existing ones.
- The new variants perform the same function as the original malware but their attributes would be so different that Antivirus software, which use traditional signature based detection, would not work on them.
- Malware classification deals with identifying the family of an unknown malware variant from a malware dataset that is divided into many families

Malware Analysis



Static Analysis

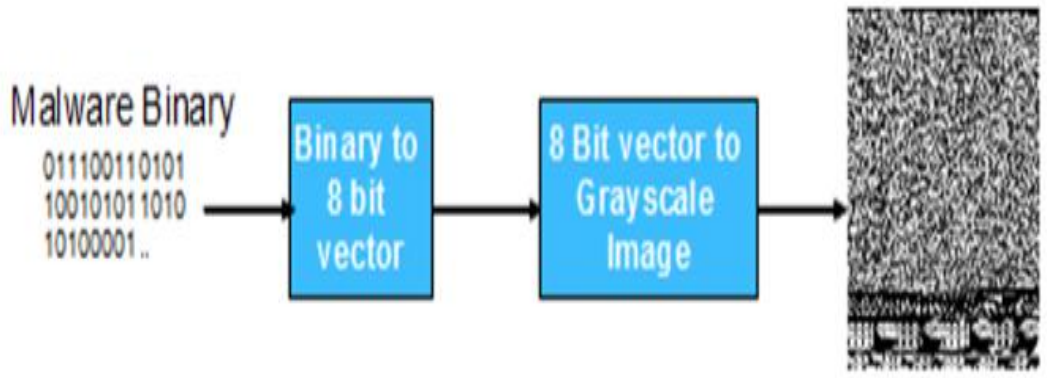
- Analyze the code and build control flow graphs
- Suffers from code obfuscation

Dynamic Analysis

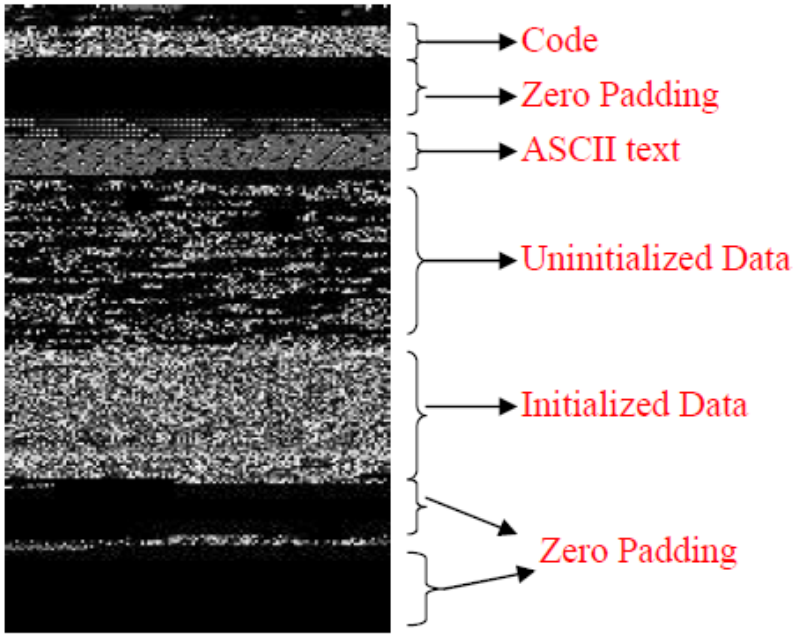
Execute the malware in virtual environment and analyze its execut-ion trace

Promising but complex and time consuming

Malware as Images



- WHY GO FOR IMAGES ?
- Different sections of a binary can be easily seen when viewed as an image



- Malware coders change small parts of the original source code to produce a new variant.
- Images can capture small changes yet retain the global structure.
- Hence, malware variants belonging to the same family appear very similar as images. These images are also distinct from images of other malware families.

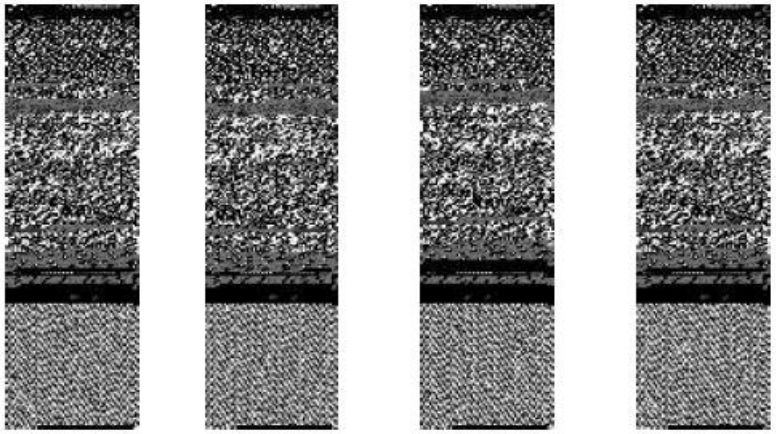


Fig: All variants of Dialplatform.B

Hands-on tutorial on how to represent malware as image and applying classical machine learning and deep learning architectures?