

Signature Based Malware Detection

Topic: Signature Based Malware Detection

Group Members:

1. Kirtiraj Chonage (2021BCS067)
2. Tanvi Rathod (2021BCS051)
3. Rahul Chormare (2021BCS071)

Abstract:

In today's digital landscape, malware continues to pose significant threats to information security, necessitating robust detection mechanisms. This project focuses on developing a signature-based malware detection system, which identifies malicious software by comparing code signatures and patterns to a known database of malware signatures. The system operates by scanning files and monitoring processes, detecting malware based on predefined signatures associated with known various known types of threats.

By leveraging pattern matching, the solution is able to detect previously identified malware efficiently and with high accuracy. Although signature-based detection excels at identifying known threats, it also highlights the importance of regular signature updates to maintain its effectiveness against evolving malware.

This project aims to provide a reliable, real-time malware detection framework, offering swift identification and alerts to prevent potential damage. Future work will explore combining this method with heuristic and behavioral analysis to counteract new and unknown malware variants.