MALWARE DETECTION AND CLASSIFICATION

TEAM I’D: 2.4

TEAM MEMBERS:

- SAIRAM B
- MRIDHULA S
- SHIVANI NARAYAN
- VEEKSHITHA

Abstract:

Malware, malicious software designed to infiltrate and harm computer systems, continues to pose a significant threat to cybersecurity. As technology advances, so does the sophistication of malware, making it imperative to develop robust methods for its detection and classification. This project aims to address this pressing concern by proposing a comprehensive approach to malware detection and classification.

The primary objective of this project is to design and implement an efficient and accurate malware detection system that can identify and classify various types of malware. To achieve this, we will employ a combination of machine learning techniques, data analysis, and signature-based methods.

Our approach involves collecting and curating a diverse dataset of malware samples, including viruses, worms, Trojans, and ransomware. We will then extract relevant features and develop machine learning models capable of distinguishing between legitimate software and malicious code. These models will be trained on the labeled dataset and fine-tuned to achieve optimal performance.

Furthermore, we will explore advanced techniques such as deep learning and behavior analysis to enhance the accuracy of our detection system. Real-time monitoring and anomaly detection will also be incorporated to detect previously unseen or zero-day malware threats.

Ultimately, this project aims to contribute to the ongoing efforts to safeguard computer systems and sensitive data from the ever-evolving landscape of cyber threats. By developing a robust malware detection and classification system, we intend to enhance the security posture of organizations and individuals, thereby mitigating the risks associated with malware infections.