PMAS Arid Agriculture University, Rawalpindi

API Based Intelligent Malware Detection

Our interconnected world is experiencing an increasing number of sophisticated cyber-attacks, which pose significant threats to individuals and organizations alike. To address this issue, we have developed a revolutionary model that classifies malware based on its behavior. We use advanced machine learning algorithms and data analysis techniques to extract features from malware reports and compile a comprehensive database of unique traits that can be used to identify different types of malwares.

We then analyze the APIs of different malware types using a sophisticated algorithm capable of distinguishing subtle variations in code. Through careful analysis, we gain a nuanced understanding of how different types of malwares behave and how they can be classified. We train our model based on the extracted APIs using a combination of supervised and unsupervised learning techniques, ensuring its performance is optimized to accurately identify different malware types. Once the training process is complete, our model analyzed the APIs of new malware samples, and quickly and accurately identifying their behavior and classification. This capability is crucial in combating cyber-attacks, enabling individuals and organizations to safeguard against the latest threats, and stay ahead of the attackers.

Overall, our model represents a significant breakthrough in the field of cybersecurity. By utilizing advanced machine learning and data analysis, we have developed a tool that can help combat the increasingly sophisticated and dangerous cyber threats facing us today. We are confident that our model will play an essential role in shaping the future of cybersecurity, and we look forward to continuing to refine and improve it in the coming years.