The research has focused on the type of objects referenced in handle tables. This details column provides in-depth information about objects which are accessed by the process and the file path to which a handle is opened. By extracting the handle information for all the process used by the two class of software able to capture the behavior activity of software and can be used to detect malware. As malware uses resource differently from benignware and this fact can be used to train classifier to categorize process as malicious or benign. The difference in number of handles usage of **section handle** by benign and malicious software explains the difference in the used by the malware is more than of benignware similarly the number of **process handle** used by the software is another indicator of maliciousness, also **mutant** are objects that can also help to distinguish between benignware and malware.

The proposed method utilizes **machine learning techniques** to create behavioral profiles for legitimate and malicious software. These profiles are built by analyzing a variety of dynamic features, such as system calls, network traffic, file access patterns, and process execution sequences. By training a classifier on these behavioral profiles, the system can effectively distinguish between benign and malicious software. This paper basically focuses on components that are highlighted like data collection, feature extraction, and the training process which comes under behavior-based detection by selecting relevant features that capture the essence of malware behavior while minimizing false positives.

*Conclusion:*

*“A Behavior-Based Approach for Malware Detection offers an effective method for detecting malware by analyzing the behavioral characteristics of software programs. This paper research contributes to the field of cybersecurity by addressing the limitations of traditional detection methods and providing a more adaptive and dynamic approach to malware detection using behavior and machine learning technique.”*

**Note:**

**In this paper the exact machine learning algorithm or technique for training the classifier is not cover**