WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Malware Scanner: A Lightweight Hybrid Detection System for Modern Threats

K. Manoj, B. Saikiran, V. Bhargav

Department of Computer Science and Engineering (Cybersecurity), Siddhartha Institute of Technology & Sciences, JNTU Hyderabad, India

ABSTRACT

In today's interconnected world, malware remains a major threat to digital infrastructure. This paper presents the design and development of a lightweight malware scanner that combines signature-based detection and heuristic analysis to identify and neutralize both known and emerging threats. The system supports real-time protection, customizable scan options, and an intuitive interface. Our goal is to provide an accessible, efficient solution for malware mitigation with minimal system overhead.

Keywords: Malware Detection, Heuristic Analysis, Signature-Based Detection, Cybersecurity, Real-Time Protection, Threat Mitigation

1. Introduction

Malware—short for malicious software—includes viruses, Trojans, worms, spyware, and ransomware that can compromise system integrity and user privacy. Existing antivirus solutions are often bulky or limited to known signatures. This project introduces a compact scanner that integrates heuristic detection to address previously unseen threats while providing usability and speed.

2. Related Work

Traditional malware scanners heavily rely on signature databases

[1]. While effective against known threats, they fail to detect new or polymorphic malware. Heuristic approaches attempt to bridge this gap by analyzing file behavior

[2]. Our project merges these two techniques in a unified system.

3. System Design

The malware scanner consists of four core modules:

- Scanning Engine: Performs signature-based and heuristic checks.
- Threat Database: Regularly updated with known malware signatures.
- User Interface: Simplified dashboard for launching scans and managing threats.
- Quarantine Manager: Isolates suspicious files to prevent system damage.

4. Implementation

The application supports three scan modes:

- Quick Scan: Targets common infection points.
- Full Scan: Thorough examination of all system files.
- Custom Scan: User-defined directories or devices.

It is built for Windows 10/11 platforms using .NET Framework and supports both manual and scheduled scans. The scanner can detect threats using file hashing, string pattern recognition, and YARA rules. Heuristic detection is implemented via behavioral pattern analysis.

5. Results and Discussion

During testing on sample datasets containing known malware and benign files, the scanner demonstrated:

- Detection Accuracy: ~95% for known threats; ~82% for heuristic detection

- Resource Usage: Consumed <150 MB RAM during full scan

- Scan Duration: Quick (~2 mins), Full (~15–20 mins), Custom (varied)

These results indicate a strong balance between performance and efficiency, especially for low-resource systems or users needing lightweight protection.

6. Conclusion and Future Work

This malware scanner offers a practical solution for detecting modern threats using a hybrid approach. It demonstrates robust detection capabilities with minimal resource usage. Future improvements may include:

- AI-based anomaly detection

- Cloud-based threat updates

- Cross-platform support for Linux, macOS, and mobile systems

References

[1] Kaspersky Labs, “Understanding Malware Signatures,” 2022.

[2] [2] S. Kaur & A. Sharma, "A Review on Malware Detection Techniques," IJCSIT, 2019.

[3] [3] M. Christodorescu et al., “Static analysis of executables for malware detection,” ACM Transactions on Information and System Security, 2007.