🛡️ File Malware Detection – Explanation Report

Purpose:

This document explains how and why a particular `.pdf` or `.docx` file was flagged as malicious by the real-time malware detection system.

---

File Details:

- Filename: suspicious\_file.pdf

- MIME Type: application/pdf

- Entropy Score: 7.89

- Prediction Confidence Score: 92.3%

- Detection Status: 🔴 Malicious

---

Reasons for Detection:

The file has been marked as malicious based on the following indicators:

1. High Entropy Score:

- A high entropy value suggests the file may be encrypted or obfuscated.

- Entropy above 7.5 is often associated with ransomware or packed files.

2. Embedded JavaScript or Macros:

- Malicious PDFs can include hidden JavaScript to run code when opened.

- DOCX files may have harmful macros or embedded objects.

3. MIME Type Anomalies:

- A mismatch between the file’s extension and MIME type can indicate a spoofed file.

- For example, a .pdf file showing a Word MIME type could be suspicious.

4. Unusual File Size:

- Significantly large or small file sizes for the format may suggest tampering or payload packing.

5. Suspicious Filename Patterns:

- Names like “invoice\_urgent.pdf” or “document\_scan.docx” are commonly used in phishing and malware.

---

Model-Based Detection:

This system uses a machine learning model trained on real-world ransomware and malware samples. The model analyzes features such as:

- Entropy

- MIME type

- File size

- Metadata structure

- Content behavior patterns

It calculates a risk score and classifies the file as either “Safe” or “Malicious.”

---

Recommendation:

- Do not open the flagged file.

- If received via email or link, delete it immediately.

- Consider scanning your system with antivirus software for safety.

---

This report is auto-generated by the real-time file scanning system to help identify and prevent malware threats.