Malware Classification and Analysis Report

Introduction

Malware refers to malicious software designed to disrupt systems, steal data, or gain unauthorized access. With the increasing use of digital platforms, malware attacks have become more frequent and sophisticated. This report studies different types of malware, analyzes malware samples using VirusTotal, observes malware behavior, and explains their lifecycle, spread, and prevention methods.

---

1. Types of Malware

Virus:

A virus attaches itself to legitimate files and spreads when the infected file is executed. It can corrupt data and slow down system performance.

Worm:

A worm is a self-replicating malware that spreads automatically through networks without user interaction, often exploiting system vulnerabilities.

Trojan:

A trojan appears as a legitimate application but performs malicious activities in the background such as data theft or creating backdoors.

Ransomware:

Ransomware encrypts files or locks systems and demands payment to restore access, causing serious financial and operational damage.

---

2. Malware Sample Analysis Using VirusTotal

Known malware hashes were submitted to VirusTotal to safely analyze malware samples. VirusTotal scans hashes using multiple antivirus engines and threat intelligence sources to identify malware type, threat level, and known behavior without executing the malware.

---

3. Detection Report Analysis

The detection reports showed varying detection rates depending on malware type and age. Ransomware samples generally had high detection ratios, while some trojans showed partial detection due to obfuscation techniques. This highlights the limitations of single-engine detection systems.

---

4. Malware Behavior Indicators

Common behavioral indicators observed included unauthorized file modifications, registry changes for persistence, communication with command-and-control servers, and attempts to disable security services. Behavioral analysis is crucial for identifying advanced and unknown malware.

---

5. Malware Lifecycle

Malware typically follows a lifecycle that includes creation, distribution, execution, persistence, command-and-control communication, and execution of malicious objectives such as data theft or encryption.

---

6. Malware Spreading Techniques

Malware spreads through phishing emails, malicious attachments, infected software downloads, removable media, and exploitation of unpatched vulnerabilities. Social engineering plays a major role in successful malware infections.

---

7. Prevention and Mitigation Methods

Malware can be prevented by keeping systems updated, using reliable antivirus solutions, enabling firewalls, avoiding suspicious links, performing regular data backups, and educating users about cybersecurity threats.

---

8. Summary and Findings

This study demonstrates that malware exists in multiple forms with different behaviors and attack strategies. VirusTotal analysis helps in understanding malware detection trends, while behavior-based indicators provide deeper insight into modern malware threats. A layered security approach is essential for effective protection.

---

9. Project Note: Malware Detector Using AI

Along with this malware classification study, an **AI-based Malware Detector** project was developed and uploaded on GitHub. The project uses machine learning techniques to analyze file features and classify them as malicious or benign, enabling detection of both known and previously unseen malware beyond traditional signature-based methods.