Malware Types & Behavior Analysis

Cyber Security Internship – Task 5

Analysis Tool: VirusTotal

Author: Mohammed Nihal

Abstract

This report presents a foundational analysis of malware types, their behavior, and detection methods. The objective of this task is to develop awareness of common malware threats and understand how security professionals analyze malware safely using threat intelligence platforms such as VirusTotal. No live malware execution was performed during this task.

1. Introduction

Malware is one of the most prevalent threats in modern cyber security. It is designed to compromise systems by stealing data, disrupting operations, or gaining unauthorized access. Understanding malware behavior and detection techniques is essential for security professionals. This report covers common malware classifications, behavior indicators, and prevention strategies.

2. Classification of Malware

• Virus: A virus attaches itself to legitimate files and requires user execution to spread. • Worm: A worm spreads automatically across networks without user interaction. • Trojan: A trojan disguises itself as legitimate software while executing malicious actions in the background. • Ransomware: Ransomware encrypts victim data and demands payment for decryption.

3. Malware Analysis Using VirusTotal

VirusTotal is an online threat intelligence platform that analyzes files, URLs, and hashes using multiple antivirus engines. Instead of executing malware locally, known malware hashes are analyzed to identify threat classifications, detection ratios, and reputation data. This approach ensures safe and ethical malware analysis.

4. Detection Report Analysis

A publicly known malware hash was submitted to VirusTotal for analysis. The detection report indicated that multiple antivirus engines classified the sample as malicious. Detection names and threat labels varied across vendors, demonstrating differences in signature■based detection methods.

5. Malware Behavior Indicators

Malware behavior indicators describe actions performed after execution. Common indicators include file system modifications, persistence mechanisms, suspicious network communication, and attempts to evade security controls. Behavioral analysis helps determine the intent and impact of malware.

6. Malware Lifecycle

The malware lifecycle consists of creation, distribution, execution, persistence, and impact. Understanding this lifecycle enables security teams to detect malware at different stages and apply appropriate defensive controls.

7. Malware Propagation Methods

Malware commonly spreads through phishing emails, malicious attachments, compromised websites, infected removable media, cracked software, and social engineering techniques. Human factors play a significant role in successful malware infections.

8. Malware Prevention and Mitigation

Effective malware prevention requires a layered security approach. Recommended practices include using reputable antivirus software, keeping systems updated, enabling firewalls, restricting privileges, educating users, and performing regular security monitoring.

9. Conclusion

This task provided practical insight into malware awareness and detection fundamentals. By understanding malware classifications, behavior, and safe analysis techniques, security practitioners can better identify threats and implement effective defenses. This knowledge forms a critical foundation for advanced malware analysis.