

Task 5: Malware Types & Behavior Analysis – Detailed Explanation

Introduction

This document provides a foundational overview of malware types and their behaviors. The objective is to understand how malware operates, how it is detected using online analysis platforms, and how infections can be prevented.

Malware Types

Viruses attach to legitimate files and require user interaction to spread. Worms self-propagate across networks without user action. Trojans disguise themselves as legitimate software, while ransomware encrypts data and demands payment for recovery.

Malware Analysis Using VirusTotal

VirusTotal aggregates results from multiple antivirus engines. By submitting known malware hashes, analysts can review detection ratios, file reputation, and static indicators without executing malware.

Behavior Indicators

Common indicators include suspicious file creation, unauthorized process execution, registry changes, and abnormal network connections. These behaviors help identify malicious activity.

Malware Lifecycle

The malware lifecycle typically includes delivery, execution, persistence, command-and-control communication, and potential payload actions such as data exfiltration or encryption.

Malware Propagation Methods

Malware spreads through phishing emails, malicious attachments, compromised websites, removable media, and unpatched vulnerabilities.

Prevention Methods

Effective prevention includes updated antivirus software, timely patching, email filtering, user awareness training, and regular system backups.

Conclusion

Understanding malware behavior and detection fundamentals is essential for cybersecurity. Basic analysis using trusted platforms improves threat awareness and supports proactive defense.