Task 5: Malware Types & Behavior Analysis (Basic)

Overview

This project focuses on understanding malware types and analyzing their behavior using a malware analysis tool. Malware is a major cybersecurity threat that can damage systems, steal sensitive data, and disrupt normal operations. This task builds basic awareness of malware and cybersecurity practices.

Objectives

- Understand common types of malware
- Learn how malware behaves after execution
- Analyze a malware sample using VirusTotal
- Study malware detection results
- Learn malware spread and prevention techniques

Types of Malware Covered

- Virus – Attaches to legitimate files and spreads when executed
- Worm – Self-replicates across networks without user interaction
- Trojan – Disguises as legitimate software to perform malicious actions
- Ransomware – Encrypts files and demands ransom for decryption

Tool Used

VirusTotal

VirusTotal is an online malware analysis platform that scans files, URLs, and hash values using multiple antivirus engines. It provides detection results, file details, and behavior analysis.

Malware Sample Used

To ensure safety, a harmless test sample was used for analysis.

- Sample Name: EICAR Test File
- MD5 Hash: 44d88612fea8a8f36de82e1278abb02f

Analysis Summary

The malware analysis was performed by submitting the hash value to VirusTotal. The results showed that most antivirus engines successfully detected the test malware. Behavior analysis provided insights into typical malware activities such as file modification, persistence, and external communication.

Malware Spread Methods

- Phishing emails
- Malicious downloads
- Infected USB devices
- Fake software updates

Prevention Techniques

- Keep operating systems and software updated
- Use antivirus and firewall protection
- Avoid suspicious links and attachments
- Regularly back up important data

Conclusion

This task helped build foundational knowledge of malware types and demonstrated how malware analysis tools like VirusTotal are used. It also highlighted the importance of preventive cybersecurity practices.

Prepared by

SAFFIQMOHAMMED S