Lab: Anatomy of Malware

Group 1

ISC 6020

Lab Objectives

The objective of this lab is to research and analyze different types of malware, understand how they work, how they are transmitted, and the impact they cause.

Background / Scenario

Malware, short for malicious software is a collective term for various forms of harmful software designed to infiltrate, damage, or gain unauthorized access to computer systems. These include viruses, worms, Trojans, ransomware, spyware, adware, and more. The purpose of malware can range from data theft and system disruption to surveillance, espionage, and even physical sabotage.

Modern malware has evolved beyond targeting personal computers. It now poses serious threats to critical infrastructure such as hospitals, power grids, public transportation, and manufacturing systems. Malware attacks can disable emergency response services**,** shut down electric generators**,** disrupt assembly lines**, or** cripple communication networks — with consequences that stretch beyond financial losses into matters of national security.

Cybersecurity researchers estimate that over one million new malware variants emerge daily. According to the McAfee Labs Threats Report 2024, notable trends include:

- The rise of ransomware-as-a-service (RaaS) operations enabling amateur hackers to launch sophisticated attacks.
- The evolution of multi-extortion tactics**,** where attackers steal and encrypt data, then threaten to leak it if a ransom isn't paid.
- Continued exploitation of vulnerabilities in Windows, macOS, Microsoft Office, cloud services, and IoT devices.
- A surge in fileless malware that lives in memory and avoids detection by traditional antivirus tools.
- Increasing targeting of supply chains**,** with malware inserted into trusted software updates or third-party components.

With these rapidly evolving threats, staying informed about the latest attack vectors, malware behavior, and protective strategies is essential for cybersecurity practitioners. For up-to-date intelligence, it's recommended to explore sources such as the McAfee Labs Threats Report**,** Microsoft Security Blog**,** Malwarebytes Labs, and Cisco Talos Intelligence**.**

Task: Conduct a Search of Recent Malware

Using reliable cybersecurity sources, I researched current malware threats and selected four recent examples, each representing a different type of malware: Ransomware, Trojan, Infostealer, and Adware.

1. Recent Malware Examples

a. Interlock Ransomware (Ransomware Type)

- **What it Does**: Encrypts user files and exfiltrates sensitive data. Victims are then blackmailed using a double-extortion technique—pay to decrypt, or the data will be leaked publicly.
- **Transmission Method**: Delivered using a social engineering trick called *FileFix*, where victims paste a fake address string into Windows File Explorer, which silently runs a PowerShell command that installs malware.
- **Impact**: Major disruptions to businesses and institutions including healthcare organizations and universities. Victims suffer financial loss, data breaches, and service downtime.

b. DoubleTrouble (Trojan – Android Banking Trojan)

- **What it Does**: Steals banking, email, and cryptocurrency credentials by mimicking legitimate apps and logging user input.
- **Transmission Method**: Shared via Discord as fake APK (Android application) files.
- **Impact**: Enables attackers to steal money directly from victims' accounts and compromise digital wallets, with serious financial and privacy consequences.

c. Trojan.Scavenger (Trojan / Infostealer)

- **What it Does**: Hides inside pirated game mods. Once active, it injects malicious code into the browser, steals passwords, session tokens, and cryptocurrency wallet data.

- **Transmission Method**: Distributed via ZIP files containing game cheats or mods.
- **Impact**: Compromises user accounts, exposes sensitive data, and leads to cryptocurrency theft.

d. Lumma Stealer (Infostealer Type)

- **What it Does**: Steals usernames, passwords, credit card numbers, and crypto wallet information.
- **Transmission Method**: Commonly delivered through phishing emails and malicious websites.
- **Impact**: Used in widespread attacks affecting thousands of users; leads to identity theft and financial fraud.

2. Detailed Summary of One Malware Example

Interlock Ransomware via FileFix (Ransomware Type)

Overview:
Interlock is a new form of ransomware that uses a deceptive technique known as *FileFix*. Victims are instructed to paste a specific string into File Explorer's address bar. This string is disguised as a file path but is actually a malicious PowerShell command. Once executed, it installs a Remote Access Trojan (RAT) and subsequently deploys the Interlock ransomware payload.

Transmission:
The malware spreads through social engineering. Victims are tricked into copying and pasting a fake address that silently executes code when entered in File Explorer.

Impact:

- Encrypts files and exfiltrates data.
- Victims are extorted twice—once for file decryption and again to prevent data exposure.
- Organizations like hospitals and educational institutions have been targeted, resulting in service interruptions and financial damages.

Conclusion

Malware is constantly evolving, and attackers continue to use creative methods to trick users and bypass defenses. From ransomware targeting critical systems to Trojans hiding in mobile apps

and game mods, the threat landscape demands continuous awareness and proactive security measures. Understanding the behavior, transmission, and impact of malware is a crucial step toward effective cybersecurity.

Sources

1. TechRadar Pro – Interlock Ransomware and FileFix Attack
2. TechRadar Pro – DoubleTrouble Trojan on Android
3. TechRadar Pro – Trojan.Scavenger in Game Mods
4. Microsoft Threat Intelligence – Lumma Stealer Threat Summary