Malware Behavior Analysis Report

Project: ALA 2 – Cybersecurity and Network Simulation

Subject: Computer Networks and Security (CNS)

Submitted by: Gopani Mahi A.

Institution: Gyanmanjari Innovative University

Year: 2025

1. Abstract

Malware is a collective term for malicious software programs designed to infiltrate, damage, or gain unauthorized access to systems and networks. Understanding malware behavior is critical in cybersecurity to develop effective defense mechanisms.

This report focuses on simulating and analyzing the behavior of three major categories of malware — **Worms, Trojan Horses, and Viruses** — within a controlled network environment. Using an interactive malware simulation tool developed as part of **ALA 2 CNS**, the experiment models how infections propagate, how users unintentionally compromise systems, and how security patches affect infection rates.

The goal of this analysis is to demonstrate how different malware types behave under various conditions (infection rate, patch rate, user action probability), and how preventive measures like patching and awareness can reduce overall infection spread.

2. Introduction

2.1. What is Malware?

Malware refers to software specifically crafted to disrupt, damage, or gain unauthorized access to a computer system. It exploits vulnerabilities in software, hardware, or human behavior to achieve its malicious objectives. Common types include worms, viruses, trojans, ransomware, spyware, and rootkits.

2.2. Purpose of Malware Simulation

Real-world malware testing poses severe security and ethical risks. Hence, controlled simulations provide a safe platform to understand malware behavior, network propagation, and the effectiveness of defensive strategies. The **ALA 2 CNS Malware Simulation** models virtual nodes representing computers in a network and visualizes how infections spread.

2.3. Objectives of the Analysis

The key objectives of this malware simulation are:

1. To observe how different types of malware spread within a network.
2. To analyze infection dynamics based on configurable parameters.

3. To evaluate how user actions (Trojan simulation) contribute to compromise.
4. To measure how patch rates mitigate the spread of malware.
5. To visualize infection patterns through real-time simulation data.

3. Malware Types and Behavior

3.1. Worms

Worms are self-replicating programs that spread automatically across networks without requiring user interaction. They exploit network vulnerabilities to copy themselves onto other connected systems.

Behavior Observed:

- Worms propagated rapidly through connected nodes.
- Infection rate increased exponentially with higher “worm infect rate” parameters.
- Even a small number of initially infected nodes caused large-scale infection within a few simulation ticks.
- Increasing the patch rate reduced infection speed, showcasing the importance of regular system updates.

Defense Mechanisms:

- Firewalls and intrusion detection systems (IDS).
- Network segmentation to prevent lateral movement.
- Regular security patches and updates.

3.2. Trojan Horses

Trojans disguise themselves as legitimate software, tricking users into executing them. Once activated, they may create backdoors, steal information, or download additional payloads.

Behavior Observed:

- Infection occurred only after a user “clicked” or “executed” the trojan file.
- Compromise probability was determined by the “Trojan Click Success Rate.”
- The simulation highlighted human error as the most significant vulnerability.
- Systems without awareness training or antivirus software had higher compromise rates.

Defense Mechanisms:

- User education and awareness.
- Limiting execution privileges.
- Endpoint protection and sandboxing unknown files.

3.3. Viruses

Viruses attach themselves to legitimate programs and propagate when these programs are executed. Unlike worms, they require a host file or program for execution.

Behavior Observed:

- The virus propagated moderately compared to worms but had persistent effects.
- Infected hosts gradually transitioned to a “compromised” state if not patched.
- The infection curve showed slower initial growth but longer lifespan in the network.
- Higher patch rates significantly reduced long-term infections.

Defense Mechanisms:

- Antivirus software for signature detection.
- Regular integrity checks and software audits.
- Behavior-based detection and heuristic analysis.

4. Simulation Design and Parameters

4.1. Simulation Environment

The malware simulation tool was developed using **HTML, CSS, and JavaScript**.

The simulation visualizes:

- **Nodes:** Represent computers or hosts.
- **Edges:** Represent network connections.
- **Colors:** Indicate health status (Green = Healthy, Red = Infected, Yellow = Compromised, Blue = Patched).

4.2. Key Adjustable Parameters

Parameter	**Description**	**Range**	**Default**
Worm Infection Rate	Probability of a worm infecting a neighbor	0 – 1	0.5
Trojan Click Success Rate	Probability that user executes a Trojan	0 – 1	0.4
Patch Rate	Chance of a node recovering per tick	0 – 0.5	0.15
Tick Speed	Time between simulation updates (ms)	120 – 1500	600
Network Size	Number of nodes in network	6 – 80	20

4.3. Simulation Controls

- **Start/Pause/Reset:** Controls simulation lifecycle.
- **Deploy Trojan:** Adds Trojan files to random nodes.
- **Seed Infection:** Seeds initial infected nodes.
- **Auto-Seed:** Automatically introduces new infections periodically.
- **Real-Time Statistics:** Displays count of healthy, infected, compromised, and patched systems.

5. Results and Observations

5.1. Worm Behavior Analysis

When the **Worm Infect Rate** was set to 0.8, infections spread rapidly — nearly 80% of the network was infected within 10 ticks.

At lower infection rates (0.3–0.4), the spread slowed, and the network stabilized faster after patching.

Observation: Worms thrive in unsegmented and unpatched networks.

5.2. Trojan Horse Analysis

With a **Trojan Click Success Rate** of 0.6, infection levels depended heavily on user clicks.

Manual interaction showed that even one unaware user could trigger a chain compromise.

However, enabling patching and lowering user click probability to 0.2 stabilized the network.

Observation: User awareness is as important as technical protection.

5.3. Virus Spread Analysis

Viruses showed hybrid propagation behavior. With an infection rate of 0.5, infection spread was moderate but persistent.

Unlike worms, viruses didn't spread explosively, but compromised nodes accumulated over time.

Observation: Viruses rely on long-term persistence and can be effectively countered by regular antivirus scans.

5.4. Comparative Summary

Malware Type	Spread Speed	User Interaction	Persistence	Best Defense
Worm	Very High	None	Medium	Patching, Firewalls
Trojan	Low	Required	High	User Awareness, Access Control
Virus	Moderate	Indirect	Very High	Antivirus, Regular Scanning

6. Discussion and Key Findings

- **Network topology** plays a crucial role in infection spread — denser connections lead to faster infection.
- **Patching frequency** directly reduces infection duration and limits compromised nodes.
- **Trojan success** depends primarily on human behavior — the "human factor" remains the weakest security link.
- **Real-time monitoring** using simulation dashboards helps visualize attack patterns and develop effective response strategies.

- **Hybrid malware models** (combining worm and virus behaviors) represent the most dangerous threats in modern cybersecurity.

The simulation highlighted that **preventive security strategies** — including automation, timely updates, and user awareness — are more effective than reactive responses.

7. Conclusion

The malware behavior analysis clearly demonstrates that malware spread is influenced by a combination of technical vulnerabilities and human actions.

Through this simulation, three malware types — Worms, Trojans, and Viruses — were studied to observe their propagation patterns, infection rates, and mitigation effectiveness.