Malware Behavior Analysis Report

Project Title: Malware Simulation – Behavior of Virus, Worms, and Trojan Horse
Prepared By: Bhavya Mehta
Course: Diploma in IT (5th SEM)
Date: October 2025

1. Introduction

Malware—software written to harm or exploit computers—shows up in many forms. In this study we focused on three classic types: **virus**, **worm**, and **trojan horse**. By simulating their behavior in a safe virtual environment, we learned practical lessons about how they spread and how to stop them.

This work is not about creating malware; it is about understanding behavior so defenders can design better protections.

2. Objectives

The simulation was designed to:

- Demonstrate how viruses, worms, and trojans infect systems.
- Observe propagation patterns and triggers in a controlled network model.
- Measure the effect of basic defenses (firewalls, segmentation, endpoint controls).
- Produce clear, practical guidance for strengthening security.

3. How the Simulation Was Run (Methodology)

- A simple virtual network represented several user machines and a subnet structure.
- Each malware type was modeled with safe, non-destructive scripts to mimic real behavior (replication, network scanning, or user-triggered execution).
- Tests were run with and without defenses: firewall rules, network segmentation, and endpoint checks.
- Observations recorded: infection rate, time to spread, detection difficulty, and persistence.

4. Behavioral Results — What We Observed

4.1 Viruses

- **What they do:** Attach to files or programs and spread when those files are run.
- **Trigger:** User action — opening or running an infected file.
- **Observed behavior:** Spread slowly and required user interaction to move from one node to another.
- **Impact:** Can corrupt files and slow systems. Easier to detect than trojans but still dangerous.

4.2 Worms

- **What they do:** Self-replicate and spread across networks without user help.
- **Trigger:** Network vulnerabilities, open ports, or weak services.
- **Observed behavior:** Rapid spread across the simulated network when firewalls/segmentation were disabled. In seconds, many nodes became infected.
- **Impact:** Can saturate bandwidth, crash services, and quickly reach many systems.

4.3 Trojan Horses

- **What they do:** Disguise as normal software, then open a backdoor or install payloads after execution.
- **Trigger:** Social engineering — convincing the user to install or run the software.
- **Observed behavior:** Fewer machines infected but infections were stealthy and persistent. They did not self-replicate, but once present they were hard to detect.
- **Impact:** Highest risk for stealthy data theft and long-term control.

5. Comparative Summary

Parameter	Virus	Worm	Trojan
Needs user action?	Yes	No	Yes
Spreads automatically?	No	Yes	No
Speed of spread	Moderate	Fast	Slow
Detection difficulty	Medium	Easy to notice (due to noisy behavior)	Hard (very stealthy)
Main risk	File/data corruption	Network disruption & wide infection	Stealthy compromise & data theft
Top defense	Antivirus + safe file handling	Patching, segmentation, firewall	Endpoint monitoring + user awareness

6. Security Lessons (Practical and Simple)

1. **People are the first line of defense.** Teach users how to spot suspicious downloads and email attachments. Small training reduces virus and trojan infections a lot.
2. **Keep systems patched.** Worms love unpatched services. Regular updates and quick patching close the doors worms use.
3. **Segment your network.** Breaking a big network into smaller segments stops a worm from using the whole network as a highway.
4. **Use layered defenses.** Combine firewalls, endpoint protection, and monitoring. No single tool stops everything.
5. **Detect memory-based threats.** Some malware runs only in memory. Use behavioral monitoring and EDR (Endpoint Detection & Response) solutions to catch stealthy activity.
6. **Hardening and least privilege.** Limit what users and services can do. If an account can't install software, many trojans fail to take hold.

7. Recommendations (Clear actions you can implement)

Short-term (right away)

- Run antivirus and endpoint scanning across all hosts.
- Enable strong firewall rules and block unused ports.
- Start basic user-awareness emails or quick training sessions.

Mid-term (weeks)

- Add network segmentation for sensitive departments and servers.
- Set up regular patch management with clear SLAs for critical fixes.
- Deploy centralized logging and simple alert rules for unusual network scanning or mass file changes.

Long-term (months)

- Invest in an Endpoint Detection & Response (EDR) tool that can spot in-memory threats.
- Build a routine incident response playbook and run tabletop exercises.
- Use least-privilege policies and restrict admin rights to reduce damage if a compromise happens.

8. Conclusion

The simulation clearly showed that **different malware types demand different defenses**. Worms are fast and make noise — patching and network controls help most. Viruses rely on users — training and antivirus matter. Trojans are quiet but dangerous — strong endpoint monitoring and cautious user behavior are essential.

Real-world protection requires **layers**: people, processes, and technology working together. When these layers are combined, the chance of a successful, long-term breach falls sharply.

9. References

- Simulation and observations based on the uploaded project report.
- NIST — Malware taxonomy (for background definitions).
- Industry whitepapers on endpoint detection and network segmentation.