Malware Behavior Analysis Report

Subject: Computer Network & Security (CNS)

Title: Malware Behavior Analysis Report

Prepared by: [Kalotara Raj J.]

Submitted to: [Vishakha Mem Shavani]

Department: [Information Tachnology]

1. Introduction

In today's digital era, malware has become one of the most significant threats to computer systems and networks. Malware (malicious software) refers to any program or code that is intentionally designed to harm, exploit, or disable computers, systems, or networks. It can steal data, spy on user activity, or cause operational disruptions.

Malware behavior analysis is a crucial process in cybersecurity that focuses on studying how malware operates after execution. This analysis helps security professionals understand the purpose, techniques, and potential impact of malicious code. The insights gained from this process are essential for developing effective detection mechanisms, countermeasures, and system defenses.

2. Objectives of Malware Behavior Analysis

The main goals of malware behavior analysis are:

1. **Understanding Malware Functionality:** To identify what the malware does after execution.
2. **Detection and Prevention:** To help antivirus and intrusion detection systems recognize similar threats.
3. **Incident Response:** To determine the extent of infection and assist in containment and recovery.
4. **Forensic Investigation:** To trace the source, propagation methods, and targets of the attack.
5. **Threat Intelligence:** To share insights with the cybersecurity community for future protection.

3. Types of Malware Behavior Analysis

Malware behavior analysis is generally divided into **two main approaches** — *Static Analysis* and *Dynamic Analysis*.

3.1 Static Analysis

Static analysis is performed without executing the malware. Analysts examine the malware’s code, structure, and metadata to understand its intent.
Key techniques include:

- **File Header Inspection:** Checking file type, size, and compilation details.
- **String Analysis:** Searching for readable strings such as URLs, IP addresses, or registry keys.
- **Disassembly:** Viewing the program’s assembly instructions using tools like IDA Pro or Ghidra.
- **Hashing:** Generating file hashes (MD5/SHA256) for identification and comparison.

Advantages: Safe, fast, and useful for initial triage.
Limitations: Ineffective against obfuscated or encrypted malware.

3.2 Dynamic Analysis

Dynamic analysis involves executing the malware in a **controlled environment** (sandbox or virtual machine) to observe its real-time behavior.
Key observations include:

- **Process Activity:** Creation or termination of system processes.
- **Network Communication:** Monitoring outgoing/incoming connections or data exfiltration.
- **File System Changes:** Detection of new, modified, or deleted files.
- **Registry Modifications:** Identifying persistence mechanisms.

Advantages: Reveals actual runtime behavior and system impact.
Limitations: Requires a safe environment and more resources.

4. Tools Used in Malware Behavior Analysis

A variety of tools are used for both static and dynamic malware analysis. Some of the most popular include:

Tool Name	Category	Purpose
VirusTotal	Online Scanner	Aggregates results from multiple antivirus engines
PEiD / Exeinfo PE	Static	Detects file packing and compiler information
Strings / BinText	Static	Extracts text and URLs from binary files
IDA Pro / Ghidra	Static	Disassembles and analyzes executable code
ProcMon / Process Explorer	Dynamic	Monitors file, process, and registry activity
Wireshark	Dynamic	Captures and analyzes network packets
Cuckoo Sandbox	Dynamic	Automated malware analysis in a safe virtual environment

These tools collectively allow analysts to gain deep insights into malware operations and indicators of compromise (IOCs).

5. Steps in Malware Behavior Analysis Process

The typical process of analyzing malware behavior includes the following stages:

Step 1: Environment Setup

- Create an isolated virtual machine using tools like **VirtualBox** or **VMware**.
- Disable internet access or route traffic through a controlled proxy.
- Install monitoring tools (Wireshark, ProcMon, Regshot, etc.).

Step 2: Initial Observation

- Record file properties: name, size, hash, and creation date.
- Run antivirus scans for baseline information.

Step 3: Static Analysis

- Check for strings, imports, and metadata.
- Identify if the malware is packed or encrypted.
- Review possible indicators such as domain names or suspicious APIs.

Step 4: Dynamic Analysis

- Execute malware in the sandbox.
- Monitor processes, file changes, and registry modifications.
- Capture network traffic and record unusual connections.

Step 5: Behavior Documentation

- Note all observed actions, such as dropped files, registry keys, and services created.
- Summarize the malware's objective (e.g., data theft, ransomware encryption, keylogging).

Step 6: Reporting

- Prepare a detailed report containing observations, indicators of compromise, and mitigation recommendations.

6. Case Study Example: Ransomware Behavior Analysis

Malware Name: WannaCry Ransomware

Type: Ransomware (Encrypts user data and demands payment)

Behavioral Summary:

- **Execution:** Once executed, it drops an executable and creates registry keys for persistence.
- **Encryption:** Encrypts files using AES and appends a ".WNCRY" extension.
- **Network Propagation:** Exploits SMB vulnerability (EternalBlue) to spread across the network.
- **Communication:** Contacts remote command-and-control (C2) servers for encryption keys.
- **Impact:** Locks users' systems and displays ransom notes demanding Bitcoin payment.

Mitigation Measures:

- Keep operating systems updated and patched.
- Backup critical data regularly.
- Use advanced endpoint detection systems.
- Block suspicious IPs and monitor network traffic for SMB exploits.

7. Malware Behavior Indicators (IOCs)

During behavioral analysis, several **Indicators of Compromise (IOCs)** can be collected, such as:

- File hashes (MD5, SHA-256)
- Malicious domains or IP addresses
- Modified registry keys
- Created or dropped files
- Network connections to unknown servers
- Suspicious processes or services

These IOCs help in threat hunting and in preventing future infections.

8. Challenges in Malware Behavior Analysis

1. **Obfuscation & Encryption:** Modern malware often hides its code.
2. **Anti-VM Techniques:** Some malware detect virtual environments and alter behavior.
3. **Polymorphic Malware:** Continuously changes code to evade detection.
4. **Time-Triggered Payloads:** Executes after a delay to avoid analysis.
5. **Resource Intensity:** Dynamic analysis requires significant computational resources.

9. Conclusion

Malware behavior analysis is a vital process for understanding, detecting, and defending against modern cyber threats. It enables analysts to reveal hidden behaviors, assess potential damage, and develop mitigation strategies.

Through proper static and dynamic analysis, organizations can strengthen their security posture, respond effectively to incidents, and contribute valuable intelligence to the cybersecurity community. The continuous evolution of malware demands constant updates in analysis techniques and tools, making this an ongoing and essential area of study in computer network security.