Blog 5: Malware Analysis – Dissecting Digital Threats

"Every piece of malware tells a story. Our job is to read between the lines." – Anonymous

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. It's a crucial skill in the cybersecurity field, helping analysts detect, neutralize, and prevent future infections.

Types of Malware Analysis

- **Static Analysis**: Examining the file without executing it
- **Dynamic Analysis**: Observing the file's behavior when executed in a controlled environment

Tools for Analysis

- **IDA Pro / Ghidra**: Disassemblers for static analysis
- **Cuckoo Sandbox**: For automated dynamic analysis
- **Wireshark**: Network traffic monitoring

Importance in Cyber Defense

- Helps identify Indicators of Compromise (IOCs)
- Improves antivirus and endpoint detection systems
- Supports incident response and forensics

Real-Life Cases

Malware like WannaCry and NotPetya brought down networks across the world. Malware analysts were on the frontlines, tracing infections and crafting defenses.

References:

- Malware Analysis by FireEye
- Cuckoo Sandbox