Understand Malware Lifecycle

Stage	Description
Delivery	Malware enters system
Execution	Malicious code runs
Persistence	Survives reboot
Privilege Escalation	Gains higher access
Defense Evasion	Avoids detection
C2 Communication	Remote control
Payload	Performs attack
Impact	Causes damage

Stages of Malware Lifecycle

1. Delivery

Malware is delivered to the victim system through:

- Malicious email attachments
- Fake software downloads
- Cracked or pirated applications
- Infected ZIP or DLL files

---

2. Execution

Once delivered, the malware is executed:

- User runs the infected file unknowingly
- DLL is loaded into a legitimate process
- Malware starts its malicious code execution

---

3. Persistence

Malware ensures it survives system reboots by:

- Adding startup or registry entries
- Hijacking execution flow

- Using boot or logon autostart mechanisms

---

4. Privilege Escalation

The malware attempts to gain higher privileges:

- Injects into trusted system processes
- Uses WMI and shared modules
- Escalates access for deeper system control

---

5. Defense Evasion

Malware avoids detection by:

- Detecting sandbox or debugger environments
- Obfuscating code
- Delaying execution (long sleeps)
- Masquerading as legitimate files

–

---

6. Command and Control (C2)

Malware communicates with external servers to:

- Receive commands
- Upload stolen data
- Update payloads

---

7. Payload Execution

Malware performs its main attack:

- Encrypts files (ransomware behavior)
- Steals user data
- Drops additional malicious files

---

8. Impact

Final damage caused by malware:

- Loss of data access
- System compromise
- Financial and privacy loss