

ANATOMY OF A MODERN CYBER ATTACK

Cyberattacks often follow a structured sequence. Understanding each phase helps in implementing defenses that can detect, prevent, and respond effectively.



RECONNAISSANCE

Objective: Gather information about the target's systems, networks, and personnel.

Tactics: Scanning public websites, social engineering, and probing for vulnerabilities.

Defense: Implement network monitoring and limit publicly available information.



WEAPONIZATION

Objective: Develop malware tailored to exploit identified vulnerabilities.

Tactics: Creating malicious payloads, such as infected documents or links.

Defense: Use advanced threat detection tools and regularly update security protocols.



DELIVERY

Objective: Transmit the malicious payload to the target.

Tactics: Phishing emails, malicious websites, or infected USB drives.

Defense: Employ email filtering, web content filtering, and user education.

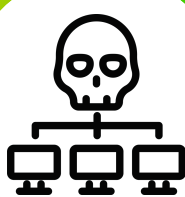


EXPLOITATION

Objective: Execute the malware to exploit a vulnerability.

Tactics: Triggering malicious code upon opening a file or visiting a website.

Defense: Keep systems patched and use intrusion prevention systems.



INSTALLATION

Objective: Establish a foothold by installing malware on the system.

Tactics: Deploying backdoors or remote access tools.

Defense: Utilize endpoint protection and application whitelisting.



COMMAND AND CONTROL

Objective: Establish communication between the compromised system and attacker.

Tactics: Using covert channels to send and receive commands.

Defense: Monitor network traffic for anomalies and block unauthorized communications.



ACTIONS ON OBJECTIVES

Objective: Achieve the attacker's goals, such as data theft or system disruption.

Tactics: Exfiltrating data, encrypting files (ransomware), or destroying data.

Defense: Implement data loss prevention tools and maintain regular backups.