Stage	What Happens?	How to Defend
Reconnaissance	Attacker gathers info	Limit public info, scan & patch
Weaponization	Creates malicious payload	Firewalls, IPS/IDS, phishing training
Delivery	Sends payload (email, USB, etc.)	Email filters, network segmentation
Exploitation	Uses vulnerabilities to gain access	Pen tests, IPS/IDS
Installation	Installs malware	PoLP, EDR, system hardening
Command & Control	Remote control established	Network monitoring, block outbound
Actions on Objectives	Attacker fulfills goals	DLP, encryption, incident response