ITEC442 IOT & Cyber Security

Week 3-4 Cyber Kill Chain

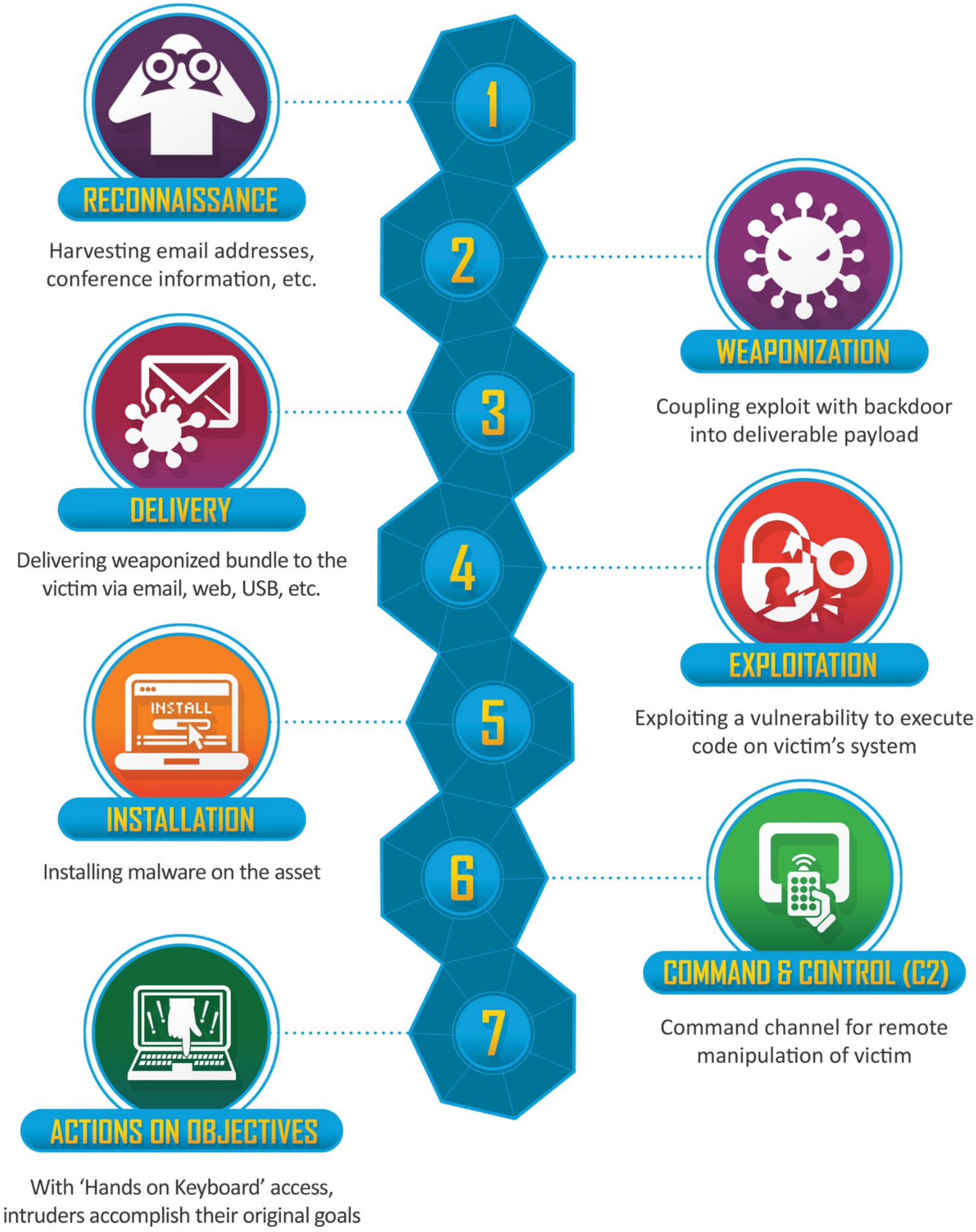
What is the Cyber Kill Chain?

The cyber kill chain is a model developed by Lockheed Martin that describes the stages of a cyber attack, from the initial intrusion to the exfiltration of data. The model is intended to help organizations understand how an attack progresses and to identify points at which they can intervene to stop the attack.

The cyber kill chain consists of seven stages:

1. Reconnaissance: The attacker gathers information about the target organization and its systems.
2. Weaponization: The attacker prepares malware or other tools for use in the attack.
3. Delivery: The attacker delivers the weaponized tools to the target organization.
4. Exploitation: The attacker uses the weaponized tools to exploit vulnerabilities in the target's systems.
5. Installation: The attacker installs tools, such as malware, on the target's systems to maintain access.
6. Command and control: The attacker establishes a communication channel with the installed tools to control them remotely.
7. Actions on objectives: The attacker uses the compromised systems to achieve their objectives, such as stealing data or disrupting operations.

By understanding the cyber kill chain and how attacks progress, organizations can develop strategies to detect and prevent attacks at different stages.



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals