Defining The Cyber Kill Chain And MITRE ATT&CK

By

Terrence Viloria

WHAT IS THE CYBER KILL CHAIN?

Lockheed Martin is credited for developing the “Cyber Kill Chain”. This model was created to track the adversary’s stages of attack to complete their mission. The model contains stages from “Recon” all the way to data exfiltration

WHAT IS MITRE ATT&CK?

MITRE Adversarial Tactics Techniques, and Common Knowledge is a knowledge base and model used for cyber adversary behavior. It reflects the various phases of an adversary's attack lifecycle and the platforms they are known to target.

Each technique contains an explanation, procedure examples, mitigation and detection. It includes metadata such as System requirements and permissions required to perform the technique.

INITIAL ACCESS

In this step, the adversary is using techniques that use various entry vectors to gain a foothold. For example, phishing

EXECUTION

This step consists of the adversary using techniques that are employed to execute malicious code on a local/remote system.

PERSISTENCE

Persistence is the step where the adversary is trying to maintain their foothold within a network or system. Techniques such as maintaining access on systems upon unexpected restarts. Ex. Adding code that executes on bootup.

PRIVILEGE ESCALATION

Privilege escalation is where the adversary is using techniques that could give them higher level of permission on a network or system. Such as having Root or Admin access.

DEFENSE EVATION

Like what the title says the adversary is trying to avoid detection. This can consist of uninstalling anti-virus and/or disabling security software or obfuscating/encrypting techniques.

CREDENTIAL ACCESS

In this step, the adversary employs techniques that lets them steal accounts and credentials such as keylogging and credential dumping. This provides them with the opportunity to create more accounts to aid them with their mission

DISCOVERY

In the discovery stage, the adversary uses techniques to gain knowledge about the targeted network /system. This aids them with useful information on further activities, targets and obstacles.

LATERAL MOVEMENT

Lateral movement is the stage where the adversary is using techniques to move through the targeted network. To achieve their mission, they often employ techniques such as pivoting through environments and multiple systems.

COLLECTION

Collection involves gathering targeted data/information to their objective. Methods include capturing keyboard input, screenshots and various target sources such as email and video.

COMMAND AND CONTROL

Also known as “C2” is the stage where the adversary use techniques to communicate with systems that have been compromised to control them.

EXFILTRATION

Exfiltration is where an adversary uses techniques that extract stolen data from the target network. Adversaries may transfer it over their C2 channel or by alternate methods such as cloud storage services.

MITRE ATT&CK USES

- Builds defenses for systems
- Monitor attack trends
- Used as a guide
- Defines threats
- Finds methods of solution
- Assesses the system/network and close gaps
- Helps plan and build your defenses
- Helps identify which group of attackers are more likely to attack your system/network

OTHER NOTES

- The goal of the defender is to keep pushing the attackers up the kill chain.
- The earlier the detection the better for the defenders.
- Red teamers use MITRE framework to test the strength of their target.
- Blue teamers use MITRE framework to understand the attacker's tactics and counter their strategy.