The Cyber Kill Chain: The Seven Steps of a Cyberattack

cyberattack and the measures you can take to prevent or intercept each step.

The Cyber Kill Chain is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives. This article describes what each of these steps entails, including the preventive measures that network defenders can take in each stage. You'll also learn how EC-Council'sCertified Threat Intelligence Analyst (C|TIA) certification can advance your cybersecurity knowledge.

1. Reconnaissance

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetrat testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third part are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline.

2. Weaponization

The weaponization stage of the Cyber Kill Chain occurs after reconnaissance has taken place and the attacker has discovered all necessary information about potential targets, such as vulnerabilities. In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target. Weaponization can include creating new types of malware or modifying existing tools to use in a cyberattack. For example, cybercriminals may make minor modifications to an existing ransomware variant to create a new Cyber Kill Chain tool.

3. Delivery

In the delivery stage, cyberweapons and other Cyber Kill Chain tools are used to infiltrate a target's network and reach users. Delivery may involve sending phishing emails containing malware attachments with subject lines that prompt users to click through. Delivery can also take the form of hacking into an organization's network and exploiting a hardware or software vulnerability to infiltrate it.

advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this process, cybercriminals often move laterally across a network to reach their targets. Exploitation can sometimes lead attackers to their targets if those responsible for the network have not deployed deception measures.

5. Installation

After cybercriminals have exploited their target's vulnerabilities to gain access to a network, they begin the installation stage of the Cyber Kill Chain: attempting to install malware and other cyberweapons onto the target network to take control of its systems and exfiltrate valuable data. In this step, cybercriminals may install cyberweapons and malware using Trojan horses, backdoors, or command-line interfaces.

6. Command and Control

In the C2 stage of the Cyber Kill Chain, cybercriminals communicate with the malware they've installed onto a target's network to instruct cyberweapons or tools to carry out their objectives. For example, attackers may use communication channels to direct computers infected with the Mirai botnet malware to overload a website with traffic or C2 servers to instruct computers to carry out cybercrime objectives.

7. Actions on Objectives

After cybercriminals have developed cyberweapons, installed them onto a target's network, and taken control of their target's network, they begin the final stage of the Cyber Kill Chain: carrying out their cyberattack objectives. While cybercriminals' objectives vary depending on the type of cyberattack, some examples include weaponizing a botnet to interrupt services with a Distributed Denial of Service (DDoS) attack, distributing malware to steal sensitive data from a target organization, and using ransomware as a cyber extortion tool.

Learn How to Prevent Cyberattacks with EC-Council