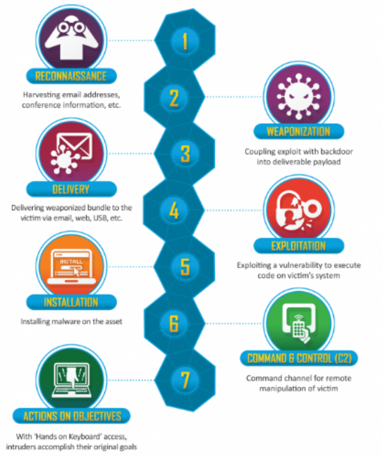
Lockheed Martin Cyber Kill Chain

The Cyber Kill Chain (CKC) framework was developed by Lockheed Martin in 2011 and it is an Intelligence Driven Defense model for the identification and prevention of cyber-attacks, specifically ones that can be classified as Advanced Persistent Threats (APTs). The CKC can help IT security teams and professionals develop strategies, products, and plans to detect and contain attacks at different stages, resulting in a more secure IT environment. In recent years, it has become the de-facto standard to describe how attacks can happen on a network. The CKC is split into seven different stages, with all seven stages needing to be completed to have a successful attack.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

KILL CHAIN STAGES

[1] Reconnaissance:

Attackers: Malicious actors will conduct research on the target organization typically using both active and passive reconnaissance methods such as domain record lookups, public IP range port and vulnerability scanning, scouting out employees on social media, and more.

Defenders: Activity conducted by the attackers at this stage will come in the format of precursors, such as IPs that are performing port or vulnerability scanning, employees being approached by individuals that they do not know, and employees potentially receiving connection/friend requests on social media.

[2] Weaponization:

Attackers: Malicious actors create their own backdoor instead of purchasing commodity malware, and host this file on a domain they own. They then write a macro within a Microsoft Word document which connects to the attacker-owned domain and downloads the malware to the system where the file was opened.

Defenders: It is extremely hard for the security team to detect this stage, as it is not happening within their environment therefore they have no visibility of what happens outside the organization (with the exception of cyber threat intelligence). Typical defenses should be employed such as anti-virus, email security, and system hardening.

[3] Delivery:

Attackers: Malicious actors have crafted a spear-phishing email using information gathered on the target from OSINT sources. The email contains a Microsoft Office document with a malicious macro that will run malware in the context of the currently signed-in user.

Defenders: The security team should have email defenses in place such as attachment sandboxing which should be able to detect any malicious attachments such as immediately malicious binaries or malicious Word documents or PDFs.

[4] Exploitation:

Attackers: Malicious actors have identified a vulnerability, that if exploited, can provide them with higher privileges than the current compromised account has, providing them with more access and the ability to perform more actions.

Defenders: The security team can prepare for this stage by hardening systems and performing vulnerability management processes to identify and remediate vulnerabilities that are both internal and externally present.

[5] Installation:

Attacker: Malicious actor installs a backdoor and deploys persistence tactics and techniques to ensure that they can keep a foothold within the infected system, allowing continuous access.

Defenders: The security team can deploy endpoint detection and response (EDR) software agents to potentially infected hosts to allow for the detection, investigation, and eradication of a malicious presence.

[6] Command and Control:

Attackers: The malicious actor installs malware that opens a channel between the malicious actor and remote machine, allowing them to send commands to the malware and attempt to gain the ability to complete step 7, actions on objectives.

Defenders: The defenders last step to fully stop the threat, prevention of command execution is key

[7] Actions on Objectives:

Attackers: The malicious actor was successful in their attack and has obtained keyboard-access, they are now able to attempt to complete any objectives they have.

Defenders: The defender must detect this stage as quickly as possible to prevent further damage and minimize the time that the attacker can complete their objectives.

IS IT OUTDATED?

Illustrating how cyber-attacks work has its issues. Attacks conducted by hackers, nation-states, and APT groups change over time and the model doesn't always show how the attack can take place. Numerous security researchers have noted that the cyber kill chain does not do a good job at describing insider threats, as well as the first two phases traditionally occurring outside of the defender's network, making it much harder to detect. In an effort to make the model work for more scenarios, MITRE combined its ATT&CK framework with the cyber kill chain to develop the **Unified Kill Chain (UKC).** The UKC consists of 18 unique attack phases that may occur during a cube attack and this includes things that the CKC left out; such as activities outside and within the network. Similar to the original CKC, the UKC can be used to analyze and defend against attacks that occur from APTs. So while the Cyber Kill Chain is still an important framework, others may be more appropriate.

‹ Previous Topic   Mark Complete ✓   Next Topic ›

Back to Lesson