International Security Architects United.

Working together • Working with others • Designing security.

Journal: Comparison of Lockheed Martin Cyber Kill Chain vs. Mandiant Target Lifecycle

Date: 2022

/isaunited

ISAUnited
International Security Architects

Comparison of Lockheed Martin Cyber Kill Chain vs. Mandiant Target Lifecycle

Introduction

Cyber-attacks have costly impacts on affected organizations, with the cost of a successful data breach amounting to $4.35 million in 2022, a 2.6% increase from 2021[1]. As the cyber threat landscape continues expanding and evolving rapidly, many companies face the uphill task of detecting and stopping attacks in their IT deployments. Some of the leading challenges include gaps in resource availability and the need for reliability of threat investigative capabilities. Attackers often leverage techniques like using a proxy server to mask their identities and hide communications to evade detection. As a result, an organization may take an average of 280 days to identify and stop an attack[2]. Therefore, it is essential to understand some of the proven methods for detecting and stopping an attack in various stages. The primary ones are the Lockheed Martin Cyber Kill Chain and Mandiant Target Lifecycle.

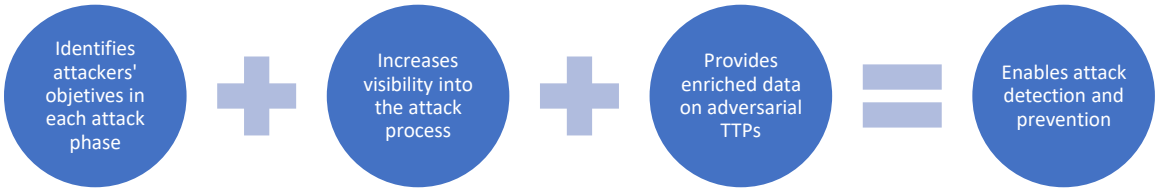
[1] https://www.ibm.com/reports/data-breach
[2] https://www.websiterating.com/research/cybersecurity-statistics-facts/

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objective

An Overview of the Lockheed Martin Cyber Kill Chain

The Lockheed Martin Cyber Kill Chain provides the various steps through which hackers launch attacks, furnishing information security teams with vital information for identifying, preventing, and intercepting attacks[3]. It provides a series of seven stages that attackers must complete before achieving their set objectives. It is a framework that enables an intelligence-driven defense model by identifying what attackers must achieve in each phase, thus increasing visibility into an attack process and providing security analysts with enriched data on adversarial tactics, techniques, and procedures (TTP). The Lockheed Martin Cyber Kill Chain enables businesses to protect themselves from complex attack scenarios, including ransomware attacks, phishing scams, advanced persistent threats (APTs), and other attacks that combine malware and social engineering.

[3] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



How Does it Work?

Lockheed Martin designed the Cyber Kill Chain to help companies detect and stop attacks at different stages. The cyber kill chain consists of seven core stages of an attack process, which start from the reconnaissance phase and ends at the exfiltration stage, where attackers accomplish their objectives. The seven stages are described below:

1. Reconnaissance

Every attack begins at the reconnaissance phase, where a hacker identifies potential targets and probes their systems and networks for the presence of exploitable vulnerabilities. When performing a reconnaissance, cybercriminals may perform activities like harvesting login credentials and gathering user IDs, operating system and software details, physical locations, and email addresses. These types of information can prove valuable when perpetrating social engineering or spoofing attacks. In addition, the more information acquired during the reconnaissance stage, the more the attackers can create sophisticated attacks to increase the likelihood of successful exploitation. Hackers can perform reconnaissance both offline and online.

2. Weaponization

After gathering the relevant information in the reconnaissance phase, attackers now develop an attack vector to exploit the identified vulnerabilities. The Weaponization phase involves developing sophisticated methods for delivering malicious payloads, including advanced phishing attacks or remote access malware, such as worms, viruses, and ransomware. Also, based on the identified security weaknesses, the attackers may create new malware or modify existing tools to execute specific attacks. The hackers may also create backdoors in the vulnerable targets' networks to maintain access in case network administrators identify and close their original entry points.

3. Delivery

Attackers now use weaponized programs and attack methods to infiltrate vulnerable systems and networks and compromise users, devices, accounts, and other assets in the enterprise technology stack. The delivery phase may involve actions like exploiting unpatched vulnerabilities, compromising outdated software and hardware, or sending malware-laden phishing emails to unsuspecting users. The specific delivery method depends on the attack type the attackers want to execute, and they may combine multiple strategies to increase effectiveness.

4. Exploitation

The programs weaponized using malicious code and delivered to the target network or system execute at this stage. Once exploited, attackers can now perform various actions on the compromised network, including installing new malware and moving laterally on the network to identify and exploit other vulnerable devices.

5. Installation

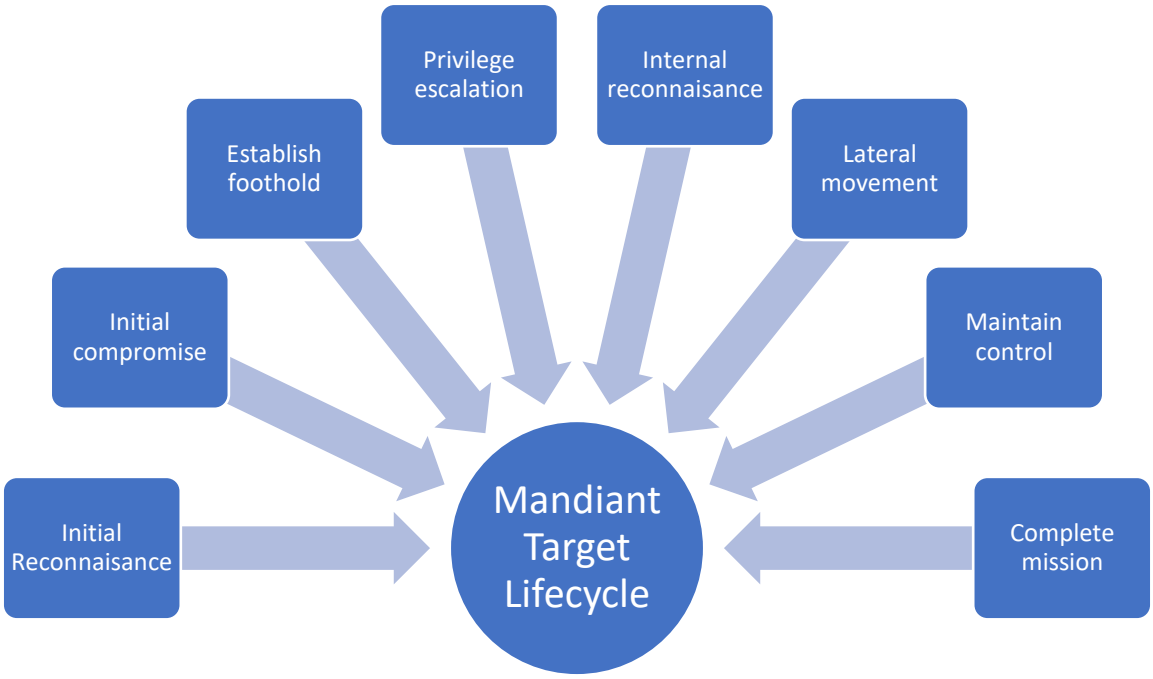
Exploiting existing security weaknesses paves the way for installing various types of malware and other attack vectors. At this point, the compromised target is at the attackers' mercy since they have already established a foothold on the network and can assume control of various network resources and activities.

6. Command and Control

Attackers use the installed malware to assume and maintain remote control of the compromised network or identity or device within the network. They can use a remote command and control server to instruct the malware to do any actions, including spying on network activities and exfiltrating sensitive data.

7. Actions on Objectives

This is the final stage of the cyber kill chain, where attackers proceed to complete their objectives. For example, they may execute ransomware attacks, use a botnet to launch DDoS attacks, steal data, or destroy critical infrastructure.



Overview of the Mandiant Target Lifecycle

It is similar to the Lockheed Martin Cyber Kill Chain, where an eight-step attack lifecycle enables organizations to determine an attack's predictable sequence of actions to identify and stop the attack at different stages[4].

1. **Initial reconnaissance:** Hackers perform extensive research on the target's systems, networks, users, and technologies to inform an intrusion methodology.
2. **Initial compromise:** Attackers use phishing methods or exploit vulnerabilities in internet-facing technologies to execute malicious code and achieve initial compromise.
3. **Establish a foothold:** the attacker may create backdoors on the compromised assets or download additional resources to assume and maintain control.
4. **Escalate privileges:** The hackers may use activities like subverting authentication systems, credential harvesting, and keystroke logging to escalate privileges and obtain additional access to more corporate systems.

[4] https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

5. **Internal reconnaissance:** The attackers investigate the company's environment to understand better the data, infrastructure, and user roles and responsibilities.
6. **Lateral movement:** With the escalated privileges and information gathered during the internal reconnaissance phase, hackers can move laterally across the compromised network environment to compromise additional systems, access network file shares, execute malicious commands remotely, and compromise remote access protocols.
7. **Maintain control:** The attackers may create numerous backdoors or leverage remote access services to assume control and maintain a presence in the compromised environment.
8. **Complete mission:** The attackers can now complete their mission, which may include stealing sensitive information, disrupting vital services or systems, or destroying critical assets.

Are they Similar?

The Lockheed Martin Cyber Kill Chain and the Mandiant Targeted Attack Lifecycle are very similar. They describe the sequential steps involved in an attack process to assist companies in detecting and stopping an attack in its early stages. Understanding the primary stages of an attack assists in developing a preventive plan to reduce and mitigate cyber risks. The Lockheed Martin Cyber Kill Chain and the Mandiant Targeted Attack Lifecycle seek to provide the following roles in cybersecurity:

- Identify attackers in each stage of an attack to enable the application of threat intelligence throughout the threat lifecycle.
- Prevent hackers and unauthorized users from accessing critical data and infrastructure assets.
- Prevent hackers and unauthorized users from sharing, saving, encrypting, or altering sensitive data.
- Enable security teams to identify and respond to an attack during the early stages to reduce impacts and effects.
- Preventing attackers from moving laterally in a network.

Do You Use Them Together or Independently?

The earlier a company can detect a threat and stop it from spreading, the less risk it assumes. That said, it is essential to use both plans together. For example, the Lockheed Martin Cyber Kill Chain misses an essential step – privilege escalation – where attackers attempt to expand access to other resources upon successful exploitation. In contrast, the Mandiant Target Lifecycle does not identify the Weaponization stage. As a result, using both methods to detect attacks in the early stages is more effective and can lead to more successful attack detection and identification.

ISAUnited
International Security Architects

Conclusion

Do you know what your enterprise architecture looks like as threats accelerate and emerge around us? Does your organization audit its attack surface - authentication and authorization, data flow, entry points, ports, SaaS, IaaS, and PaaS integrations, internet-facing assets, and more to keep your architecture, infrastructure, and people safe? ISA United encourages organizations to conduct attack surface analysis by reviewing your architecture and infrastructure. Conducting threat models and creating threat maps of what technical components and systems need to be reviewed and tested for security vulnerabilities. Curate the technical security controls you need to mitigate the risks. ISA United group of experts recommend that you apply the Lockheed Martin Cyber Kill Chain and Mandiant Target Lifecycle to identify attacks in your architecture early and deploy robust security controls to protect your organization.