The Defensive Methods for Cyber Kill Chain

Ms. Ananya Sathyanarayanan
Post Graduate Cybersecurity Student, Faculty of Computer Application Department, Marwadi University, Rajkot
Email: ananya.s.2906@gmail.com
Dr. Ravirajsinh Vaghela
Assistant Professor, Faculty of Computer Application Department, Marwadi University, Rajkot
Email: ravirajsinh.vaghela@marwadieducation.edu.in

ABSTRACT

Cyber kill chain is an integral part of cybersecurity. Cyber Kill Chain is an intrusion- centric model, which explains about the different stages of a cyber-attack. The kill chain is setup to illustrate the active state of a data breach throughout the different phases. User behavior analytics helps to prevent and halt ongoing attacks before any damage is done by enhanced threat intelligence at every phase of the Cyber Kill Chain. In this paper, we have discussed various mitigation steps to interrupt and break the chain at each phase. Thus, this will help us to stop an attack from becoming successful.

Keywords – **Cybersecurity, Cyberweapons, Cyber Attack, Cyber Kill Chain, Hacking, Networking, Vulnerability, Threat**

1. INTRODUCTION

Tools such as IDS, firewalls, and antivirus software are examples of traditional network protection systems that leverage static knowledge of current system threats and vulnerabilities. Such a strategy enables us to watch as computer attacks become more and more successful and extraordinary data leaks occur. Traditional strategies no longer work due to the sophistication of the instruments used by hackers and the growth of their objectives [1]. However, there isn't a corresponding model from a defensive perspective, meaning there isn't a predictable pattern of steps for the accurate detection of threats [2]. Network defensive strategies that make use of adversary intelligence, threat modelling, and attack scenarios can drastically lower the likelihood of each attack attempt. The computer incident response team (CERT / CSIRT) can more quickly identify participants in the anti-organization campaign and establish the directions and means of defense by using the kill chain model to better understand the purpose and tactics of assault. The evolution of contemporary attacks necessitates a change in the defense paradigm to one that is based on threat information and emphasizes threats as well as vulnerabilities. The use of AI will likely continue to be most obvious in the near future during the different phases of cyber kill chain [3]. of It is crucial to protect not only the system's weak points or the system, but also to defend the system against all threats—known and unknowable—independently of the system's vulnerabilities. In this paper, we will discuss about the Cyber Kill Chain steps and the ways to mitigate it at each level. Also, a set of generalized good practices will be explained for each phase to reduce and mitigate it in future.[4]

2. HOW CYBER KILL CHAIN WORKS?

Cyber Kill Chain model was created by Lockheed Martin order identify, capture & trace the stages of Cyber Attack which in turn will help the security professionals to mitigate the attack at various stages of the chain mode. The idea of using the term Kill Chain was inspired from the army, as they use it to describe the assault of an organization [4].

A successful attack involves a series of steps, starting with the identification phase, where the main goal is to gather information about the victim. This can be done by using social engineering techniques, hacking, tampering their two-way data flow in the computer network, use of malware and infection of the system control. We can examine each of these occurrences, learn from them, and utilize that knowledge to disrupt the chain at the earliest. We can discover more about the attackers, the more thoroughly we examine these incidents. The key to defense becomes more accurate when detection is done precisely.

Cyber Kill Chain follows 7 distinct steps: [3]

2.1 Reconnaissance

This is the first stage which takes place in kill chain model. This stage mainly involves gathering and learning as much as possible about the potential victims before attacking them. During this phase, the potential targets will be identified, their weakness will be discovered, their current and new entry point will be deeply analyzed, etc. this phase can be investigated both in online and offline [5].

2.2 Weaponization

Cyberweapons and as well as other tools are utilized to break into a victim's network and disrupt their system during the delivery stage. Sending phishing emails with malware attachment and clickbait subject's lines to victim's is an example of Delivery. Breaking into a company's network and infiltrating it using a hardware or software weakness is also a form of Delivery Stage.

2.3 Delivery

Cyberweapons and as well as other tools are utilized to break into a victim's network and disrupt their system during the delivery stage. Sending phishing emails with malware attachment and clickbait subject's lines to victim's is an example of Delivery. Breaking into a company's network and infiltrating it using a hardware or software weakness is also a form of Delivery Stage [6].

2.4 Exploitation

The phase that comes after delivery and weaponization is exploitation. Hackers use the vulnerabilities they have identified earlier phases during exploitation stage to further dive deep into a target's network and achieve their goals. Cybercriminals frequently traverse networks laterally throughout this procedure to reach their objectives. Occasionally, exploitation might direct attackers to their intended targets if network administrators have not implemented deception techniques.

2.5 Installation

Cybercriminals attempt to install malware and other cyberweapons into the victim's network to seize control of the system, steal sensitive information and critical data during the installation phase of Cyber Kill Chain. Attackers will use backdoors, Trojan horses, command-line interfaces in this step to install malware and other cyber weapons.

2.6 Command and Control

Cybercriminals interact with the malware they have planted on a victim's network in the C2 Stage of Cyber Kill Chain to give instructions to the tools so they will accomplish their goals. For instances, attackers will use the C2 servers to command computers to execute the cybercrime goals or communication channels to instruct systems infected with the botnet malware to flood the website with DDoS attack.

2.7 Action on Objective

Cybercriminals start the final phase of the Cyber Kill Chain, executing the goals of their cyberattack, after creating cyberweapons, installing them on a victim's network, and seizing control of that victim's network. The ultimate fact is that the goals of cybercriminals differ depending on the type of cyberattack. For example, it can be disseminating malware to capture sensitive information for an organization and applying ransomware as a means of Cyber extortion.

3. PREPARATION TO DEFEND THE CYBER KILL CHAIN

Analyzing and learning for how a computer undergoes an attack can be of a great advantage to the security department in any company. To start, we can consciously design a security architecture to pinpoint attacks and locate the place of the plan's attack. This will make choosing of the defense tools & procedures much easier. The main objective is to interrupt the Kill Chain at any point of the stage, with the exception for the last stage, where the system is breached, and the data i s compromised.

It is vital to setup the infrastructure so that the security requirements can stop or impede the attack. The techniques of Defense of Depth & Security by design can be applied here. We should setup the infrastructure to defend against attacks in the broadest feasible variety of attack types and using the company's methods. Setting objectives for the performance of tools, procedures, rules, and policies is crucial when creating a defensive infrastructure architecture [9].
Tasks to keep in mind when preparing the defense model [10]:

3.1 Detect

This simply means to detect an attack. To neutralize an attack, it is important to recognize the attack and appropriately diagnose the situation. It is reasonable to conclude that this is the security system's most crucial feature from a defense standpoint.
Tools & Techniques: HIDS, Firewalls, SIEM, File Integrity Control.

3.2 Disrupt

This simply means to disrupt or interrupt the attack. By deploying some technical solutions, we can hinder a computer attack to a great extent. We can substantially reduce the attack's effectiveness.
Tools & Techniques: Honeypots, Honey nets.

3.3 Deceive

Deceive means to trick the attacker into the attack. In this, the attacker is shown false presumptions about the system, which will force the attacker to select an unproductive attack vector, thus the deception effect is created.
Tools & Techniques:Honeypots, obfuscation of application code, incorrect server, or configuration information.

3.4 Degrade

Degrade means weaking of an attack. It involves reducing the strength of the attack, and as a result its efficiency. Although the attack is carried out, its effects on the organization are minimal.
Tools & Techniques: tarpit, short time leads, time limitation.

3.5 Prevention

This means defending against an attack. The goal of this phrase is to prevent an attack. Tools & Techniques: IPS, Access Control List (ACL), whitelisting, sandboxing.

Fig 1: Cyber Kill Chain Process [8]

4. MITIGATE & INTERRUPT THE ATTACK CHAIN (PROPOSED WORK)

The Cyber Kill Chain could theoretically be broken at any phase. The most common way to break the chain is by proactive and ongoing monitoring of engagement with system data and information. For instance, if real-time warnings show that permissions are being elevated, we can act right away to stop the attacker from accessing confidential data.

	• IPS | Firewall | DLP | Document Security • Threat Intelligence
Delivery	• Firewall | Anti-Spam | URL Filterring | Threat Emulation | Threat Extraction
Exploitation	• Anti-Virus | IPS | Threat Emulation
Installation	• Anti-Bot | Endpoint Security
Command & Control	• Anti-Bot | Endpoint Security | Forensics | Mobile Threat Prevention
Action on Objective	• DLP | Document Security | Firewall | IPS

Table 1: Techniques to mitigate Cyber Kill Chain

You might even be able to identify risks during the reconnaissance phase in some circumstances. You can quickly stop a user from accessing a file containing confidential information if they do so for the first time and you believe they shouldn't. this could completely avert a threat from arising. The following are the effective methods for how to break the Cyber Kill Chain [2, 8].

4.1 Mitigate at Reconnaissance

In order to mitigate reconnaissance, the first step is to obtain the website visitor logs for the purpose of finding historic data and modifying. It is good to engage with the website administrators to make use of their current browser analytics. As reconnaissance is the initial step for any detection to take place, it is good develop detection for reconnaissance - specific browsing behaviors. Continuously examine network traffic flows to find and stop host sweeps and port scans. Always prioritize certain technology or individua
ls at the top of the list for protection depending on reconnaissance activity. Lastly, create security awareness training so users are aware of what should and shouldn't be posted, such as private information about customers, event attendees, job titles and duties, etc [11].

4.2 Mitigate at Weaponization

To mitigate at weaponization, always examine relationship between the creation and use of malware over time. Identifying which APT Campaigns use which weaponizer artefacts. While the new malware may be active with customized operations, the old malware typically mean it comes off the shelf. Conduct malware analysis, also on the process of creation along with the malware payload. This helps us find the origin of malware. It is also good to gather files and metadata for future use in digital forensics. Lastly, always organize training on security awareness [11].

4.3 Mitigate at Delivery

One of the basic steps to mitigate at delivery is to evaluate the delivery method to determine how the target systems are affected. Also identify the date and time of the day the attack started. We can use targeting to infer the enemies' intentions. Gather details about the roles and duties of the individuals on the targeted servers as well as the confidential material they have admin rights to. Always make use of weaponizer artefacts to spot fresh malicious payloads at the delivery point. Lastly, even if an intrusion is discovered after it has already happened, you must be able to tell when and how the distribution started by gathering the email and wen logs for forensic reconstruction.

4.4 Mitigate at Exploitation

The initial step to mitigate at exploitation to restrict admin privileges and custom endpoints. These are the examples of endpoint hardening techniques that prevent the execution of shellcode. It is recommended to always audit endpoint process to forensically identify the source of the exploit. Conducting regular penetration testing and vulnerability scanning are always mandatory to keep everything in check. Block any endpoint exploitation for vulnerabilities, both known and undiscovered. It is essential to give training in secure coding for web developers. Lastly, it is good to automatically distribute fresh defenses worldwide to fend off follow-up attacks [9].

4.5 Mitigate at Installation

To mitigate at installation, identify whether malware needs administrative rights. Knowing when the malware was built will help you tell whether it is recent or old. This will help us take appropriate steps for mitigation. Always audit the endpoint processing to find unusual file creations. Obstructing the popular installation routes is always required. If there are any signed executables, they should have their certificates extracted.

4.6 Mitigate at Command and Control

Malware analysis reveals C2 infrastructure. So, keep discovering C2 infrastructure through malware analysis. It is also a good point to customize C2 protocol blocks on web proxies. Always reduce the amount of internet points of presence on your network and use proxies for all sorts of traffic to harden the network (HTTP, DNS). Configure is such a way that proxy category blocks should contain domains marked as 'None' or 'Uncategorized'. To find and stop infected hosts, redirect malicious outbound communication to internal sinkholes. Lastly, always perform open-source study to obtain fresh adversary C2 infrastructure. [9]

5. DISCUSSION

In this paper, we have discussed some of the step to mitigate cyber kill chain at each phase. If we see in reconnaissance, it is good develop detection for reconnaissance-specific browsing behaviors. While in weaponization, always examine relationship between the creation and use of malware over time. this helps us identify how active the malware is today's scenario and appropriate steps can be taken. In delivery, it is essential to make use of weaponizer artefacts to spot fresh malicious payloads at the delivery point. Finally in Command & Control, good point to customize C2 protocol blocks on web proxies.

Along with the steps to mitigate the cyber kill chain mode, we have also discussed some of the best practices methods to be followed which will enhance the security.

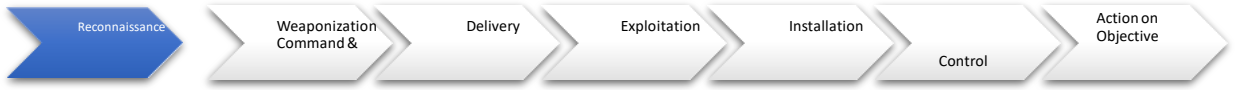

Fig 2: Mitigate at Reconnaissance

Fig 3: Mitigate at Weaponization

Fig 4: Mitigate at Delivery

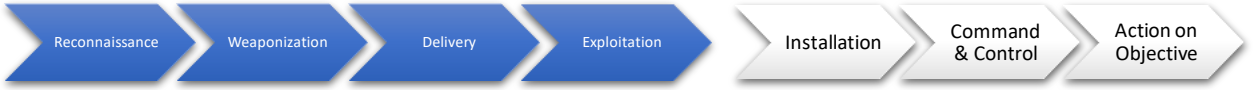

Fig 5: Mitigate at Exploitation

Many a times, it's been observed that organization do create a set of rules, policies & procedures to be followed and maintained. But, many times, some of the rules and regulations are not adhered continuously due to various internal and external factors. To begin with, if the organizat ions follow the rules & policies set by the organizations and the organizations also keep updating the security code book in accordance with the latest happening, at least the basic security can be assured. Furthermore, by following the mitigation steps explained in section 4 and inculcating them in the organization, Security Code Book can be much more effective and efficient for security organization from cyber kill attacks to a great extent.

6. CONCLUSION & FUTURE WORK

The Cyber Kill Chain is very a very effective model. It can be used for both attack and defense [14]. We can observe the attack from the offensive perspective and then create a defense against it [15]. It is necessary to put in place an integrated Cyber Protection System to be able to plan for defense against attacks. In addition to purchasing a technological solution, one should approach the creation of cyber security as a continuous process to achieve this properly and most importantly, effectively. It is essential to make use of all the information, resources, and organizational options available.

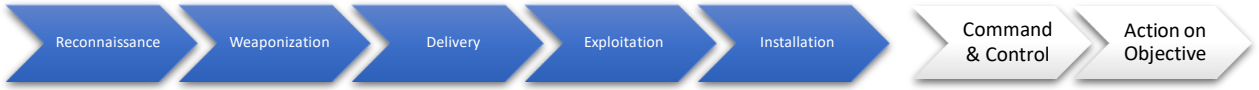

Fig 6: Mitigate at Installation

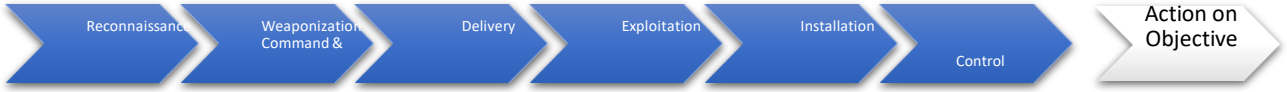

Fig 7: Mitigate at Command & Control

In this paper, we have attempted to provide solutions to mitigate Cyber Kill Chain at every phase. For all the phases we have provided the steps to interrupt the stage at the highest possible level. Also, a set of good practices to be followed and implemented are discussed. For future work, we would definitely attempt to find full-fledged technical solution to mitigate all phases of Cyber–Kill Chain.

REFERENCE

[1] EC-Council (2022) Cyber Kill Chain: The Seven Steps of a Cyber Attack Available at: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain- seven-steps-cyberattack/ (Last Accessed: 17th September 2022).

[2] Villalón-Huerta, A., Gisbert, H.M. and Ripoll-Ripoll, I., 2022. SOC Critical Path: A Defensive Kill Chain Model. *IEEE Access*, *10*, pp.13570-13581.

[3] Chomiak-Orsa, I., Rot, A. and Blaicke, B., 2019, September. Artificial Intelligence in Cybersecurity: The Use of AI Along the Cyber Kill Chain. In *International Conference on Computational Collective Intelligence* (pp. 406-416). Springer, Cham

[4] Tarnowski, I., 2017. How to use cyber kill chain model to build cybersecurity. *European Journal of Higher Education IT*.

[5] Haber, M.J. and Rolls, D. (2019) 'Identity Management Controls in the Cyber Kill Chain', in Identity Attack Vectors.
Berkeley, CA: Apress, pp. 117–124. doi:10.1007/978-1-4842-5165-2_11.

[6] Assante, M.J. and Lee, R.M., 2015. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, *1*.

[7] L. Zhang and V. L. L. Thing, "Three decades of deception techniques in active cyber defence - Retrospect and outlook," *Computers & security*, vol. 106, p. 102288, 2021, doi: 10.1016/j.cose.2021.102288.

[8] Yamin, M.M., Ullah, M., Ullah, H., Katt, B., Hijji, M. and Muhammad, K. (2022) 'Mapping Tools for Open-Source Intelligence with Cyber Kill Chain for Adversarial Aware Security', *Mathematics (Basel)*, 10(12), p. 2054. doi:10.3390/math10122054.

[9] Abi Tyas Tunggal, UpGuard (2022) What is Cyber Kill Chain and how to use it Effectively. Available at: https://www.upguard.com/blog/cyber-kill-chain#toc-1 (Last Accessed on 17th September 2022)

[10] Pratik Dholakiya (2020) What is Cyber Kill Chain?. Available at: https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain- and-how-it-can-protect-against-attacks (Last Accessed on 19th September 2022).

[11] Cyberpedia (2021) How to break the Cyber Attack Lifecycle. Available at: https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle (Last Accessed on 18th September 2022)

[12] Khan, M.A., 2021. *NADRA Database Hack In Context Of Cyber Kill Chain and Overview of Pakistan's Cyber Security* (No. 5257). EasyChair.

[13] Garba, F.A., 2019. The anatomy of a cyber-attack: dissecting the cyber kill chain (ckc). *Scientific and practical cyber security journal*, *3*(1).

[14] Cooper, M., 2022. Using the Cybersecurity Kill Chain for Attack and Defence. *ITNOW*, *64*(2), pp.38-41.

[15] Lockheed Martin (2022) Cyber Kill Chain. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Last Accessed on 19th September 2022)

Author's Profile

Ms. Ananya Sathyanarayanan is currently pursuing MSc. Cybersecurity & Cyber Law from Marwadi University, Rajkot. She has done BSc. Computer Science from Heriot Watt University, Dubai, UAE. She has been awarded with Deputy Principal Award for her Academic Excellence by Heriot Watt University. Her areas of interest are Defensive Security, Blue Teaming & Digital Forensics.

Dr. Ravirajsinh Vaghela is working as an Assistant Professor in the Faculty of Computer Application (FoCA), Marwadi University, Rajkot. He has done his Master in Computer Application branch in 2009, and completed PhD in Computer Science in 2018 under the guidance of Dr Atul Gosai. He has 11+ years of teaching and research experience. He has published 20+ research papers in various National and International Conferences, Book chapters and Journals. He holds a professional membership for CSI. His area of interest includes Machine learning, IOT, and Cyber Security.