Cyber Kill Chain and MITRE ATT&CK Framework Analysis

Phyrum Rithchea

MSc in Management of Information Systems (MIS), Paragon International University, Phnom Penh, Cambodia

*Corresponding author's e-mail: prithchea1@paragoniu.edu.kh
doi: https://doi.org/10.21467/proceedings.174.5

Abstract

This paper aims at exploring and analyzing the relationship between Cyber Kill Chain and MITRE ATT&CK framework by detailing all phases of Cyber Kill Chain model with the technical flow from the mindset of attackers, discussing all tactics and techniques of MITRE ATT&CK framework in the area of preparatory and Windows matrix in the enterprise, and leveraging and utilizing all tactics, techniques, and procedures (TTPs) in MITRE ATT&CK framework with all the phases of the Cyber Kill Chain model. By achieving this, cybersecurity analysts as well as defenders can understand and foresee attackers' mindset and perspective, especially the attackers' attack methodology and their TTPs used in each phase of the attack methodology so that the defenders are able to protect and prevent valuable and critical digital assets from being exploited and compromised by the cyber-terrorists.

Keywords: *Cyber Kill Chain, MITRE ATT&CK Framework, Cyber-terrorists*

1 Introduction

In this digital era, information security has been playing a really significant role in many aspects such as daily activities, businesses and workplaces by allowing people to communicate with each other, complete their valuable tasks, and protect their digital assets without the fear of being threatened or hacked by cyber-terrorists or cyber-criminals. Cyber Kill Chain is a framework which was developed by Lockheed Martin. It is a component of the intelligence driven defense model for detection or identification and prevention of cyber intrusion activities. This model identifies what the attackers must do in order to achieve their goals by following all the seven phases. For MIRTE ATT&CK framework, it is an open-source framework and knowledge base of attackers' tactics, techniques, and procedures based on real-world observations. This framework is used as a justification for the improvement of specific threat models and methodologies in many sectors such as private, public, and especially in information security. Many research papers only focus on Cyber Kill Chain or MITRE ATT&CK framework individually while there is lack of research paper that discusses and analyzes both of them together. Also, Cyber Kill Chain and MITRE ATT&CK framework provide useful information and knowledge about the flow of cyber-attacks and the tactics, techniques and procedures that attackers can use to exploit their target, which are very crucial for defenders to keep track of them and protect their people as well as digital assets. The primary objective of this paper is to explore and analyze the relationship between Cyber Kill Chain and MITRE ATT&CK framework on preparatory matrix and Windows matrix in order to understand and leverage what tactics, and techniques in MITRE ATT&CK can be used and implemented to what phases in Cyber Kill Chain.

2 Literature Reviews

2.1 Cyber Kill Chain

Yadav and Mallari (2016) discussed the technical aspects of Cyber Kill Chain by going through all seven phases of the framework while Tarnowski (2017) showed how to use Cyber Kill Chain model to build cybersecurity, especially to protect a data center from intruders. According to Yadav and Mallari (2016), those seven phases are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective. Also, the authors gave technical flows from attacker's perspective which may help security researcher to design prevention mechanisms. Although the authors discussed about attacks in general without consideration of operating systems or application software because Cyber Kill Chain was a process rather than a technology, technologies involved at each phase of the cyber kill chain process was analyzed without giving much detail. In Tarnowski's research article (2017), he mentioned about all seven stages of cyber kill chain and how it looked like from the attacker's perspective. Moreover, he discussed about how to prepare a defense system by giving procedures and a technical solution matrix for defense which consisted of tools and technologies that defenders could use to detect and protect their assets from being attacked. Although Cyber Kill Chain is a good security mechanism to protect as well as to defense the system from being exploited, these tasks can be carried out by other security frameworks.

Proceedings DOI: 10.21467/proceedings.174; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-984081-6-7

2.2 MITRE ATT&CK Framework

According to MITRE Corporation (2021), this organization listed and explained all tactics, techniques, and procedures (TTP) in all aspects of operating systems including mobile devices in matrices clearly whereas Al-Shaer, Spring, and Christou (2020) presented their statistical machine learning (ML) analysis on Advanced Persistent Threat (APT) and Software attack data reported by MITRE ATT&CK to assume the technique clustering that represented the meaningful correlation that could be used for technique prediction. The group of authors developed a novel approach using hierarchical clustering to infer technique associations that represented various technique interdependencies in a tactics, techniques, and procedures (TTP) chain while MITRE Corporation discussed in details about all TTPs and behaviors of many advanced persistent threat (APT) groups. Not only did it provide many information about APTs and TTPs, but it also proposed ways to avoid those potential threats and security mechanism to track and detect those threats.

In spite of discussing and detailing all TTPs of APT groups, and building a hierarchical clustering to infer those technique associations, they did not illustrate steps of how hackers can attack a targeted machine or environment. Yadav and Mallari (2016) discussed the technical aspects of Cyber Kill Chain by going through all seven phases of the framework. Tarnowski (2017) showed how to use Cyber Kill Chain model to build cybersecurity, especially to protect a data center from intruders. MITRE Corporation (2021) listed and explained all tactics, techniques, and procedures (TTPs) in all aspects of operating systems including mobile devices in matrices clearly, and Al-Shaer, Spring, and Christou (2020) presented their statistical machine learning (ML) analysis on Advanced Persistent Threat (APT) and Software attack data reported by MITRE ATT&CK to assume the technique clustering that represented the important correlation that could be used for technique prediction. However, there is no literature that discusses and analyzes both Cyber Kill Chain and MITRE ATT&CK framework together. In response to that, I think it would be a golden opportunity for me use all the existing literatures as a guide in order to fulfill a gap as well as to build another bridge for future and talented researchers to explore more in this area.

3 Cyber kill chain analysis

Cyber Kill Chain is a framework which was developed by Lockheed Martin. It is a component of the intelligence driven defense model for detection or identification and prevention of cyber intrusion activities. The model identifies what the attackers must do in order to get their goals done (Lockheed Martin Corporation, 2015). In Cyber Kill Chain, there are seven phases and they are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective phase. All of these phases are depicted in Figure 1 below.

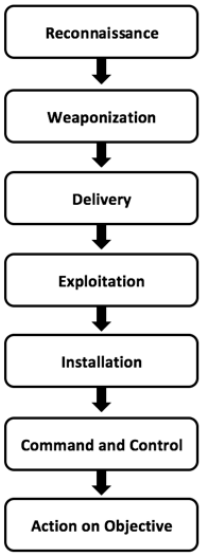

Figure 1: The Seven Phases of Cyber Kill Chain

In the first phase, it is about performing the reconnaissance. The term “Reconnaissance” means collecting information about potential targets, which can be individuals, or organizations. The goal of this phase is to collect as much information as possible about a target environment. In this phase, attackers can find, identify, determine, and choose their target by scanning the Internet, web crawling, social media, conferences, blogs, websites or using other tools such as “Nmap (Network Mapper)” to scan their target network environment in order to look for vulnerabilities and so on. Once the attackers obtain enough information about their target, they will proceed to the next phase which is the “Weaponization” phase.

In the weaponization phase, the attackers try to design and build their malicious codes or tools in order to penetrate or exploit their target machine or organization based on their information that was gathered during the reconnaissance phase. After the attackers finish building their payloads, they will send them to their target to start their attack, and this is done in the "Delivery" phase. In this phase, they send or upload their attack tools to their target environment through many means such as email attachment, USB, website, malicious links and so on. Moreover, in the exploitation phase, the payloads are executed in the attacked environment if the delivery phase is successfully achieved. It means that all the attackers' tools or malicious codes are delivered to the victim's machine properly and can be used to exploit the vulnerabilities that are present on the victim's machine. After that, a trojan horse or backdoor or malware is installed on the victim's machine which allows the attackers to visit and attack the victim's machine. And, this can be achieved in the installation phase.

Next, it is about the "Command and Control (C&C or C2" phase. When the payloads, especially the backdoors are installed on the target machine successfully, the infected victim's machine can be remotely controlled by the attackers. In this phase, the attackers are able to control their infected machines by sending any commands to them based on their goals and objectives that they want to accomplish. Finally, "Action on Objective" phase is the last phase of the cyber kill chain model. In this phase, the attackers can perform their actions such as collecting sensitive data, stealing credentials, observing or monitoring all activities, damaging or destroying the victim's machine based on their objectives. Therefore, the cyber kill chain model is really beneficial because it gives a complete overview of how a cyber-attack can be done with great details in each phase. According to Tarnowski (2017), in order to interrupt or stop the attack, it is very important to set goals for the performance of equipment, procedures, policies, and people. These tasks are detection, prevention, disruption, degradation, and deception. In the detection step, an attack can be detected by the use of tools and technologies such as Host-Based Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS), Security Information and Event Management (SIEM), anti-virus software, firewalls, well-trained users and so on. For the prevention step, the attack can be prevented by using Intrusion Prevention (IPS), scan lock, firewalls, access control lists (ACLs), penetration tests, code obfuscation, custom configurations, vulnerability and availability updates, application whitelist, sandboxing and a well-implemented information security policy.

Regarding the disruption step, the attack can be disrupted by implementing some technical solutions such as hardening systems and installing network traps which consists of honeypots and honeynets. And, in the degradation step, it consists of weakening the power of attack, and consequently its effectiveness. The tools and techniques that can be used to accomplish this task are tarpit, configuration changes to shorten session times (short lead times), policies that impede the inclusion of services (time limitation, limitation for different users). Last but not least, in the deception step, the deception effect is achieved by introducing the attacker and by forcing the wrong assumptions about the system, which will result in selecting an ineffective attack vector. Deceptive tools include honeypots, obfuscation of application code, or returning incorrect application, server, or configuration information. Therefore, the attack can be detected and managed properly by following all of these steps, setting up appropriate security controls, and having proper information security policies and procedures in place.

4 MITRE ATT&CK framework analysis

MITRE ATT&CK is an open-source framework and knowledge base of attackers' tactics, techniques, and procedures (TTPs) based on real-world observations. The ATT&CK knowledge base is used as a justification for the improvement of specific threat models and methodologies in the private sector, in public sector, and in the cybersecurity community (MITRE ATT&CK, 2021). MITRE ATT&CK framework also provides rich knowledge about the tactics, techniques, and procedures (TTPs) of attackers. In MITRE ATT&CK framework, there are two main matrices which are enterprise and mobile. In enterprise matrix, it consists of PRE, Windows, macOS, Linux, Cloud, Network, and Container matrix whereas in the mobile matrix, there are only two matrices which are Android and iOS. However, since my research study only focuses on Windows matrix in the enterprise, other matrices will not be discussed in detail and they will only be referred to as appropriate.

Before discussing the Windows matrix, it is worth knowing and understanding about the preparatory matrix which attackers can learn and understand more about their target environment. There are two tactics listed in the preparatory matrix and they are reconnaissance and resource development. For the reconnaissance, it contains techniques that involve attackers actively or passively gathering information that can be utilized to support targeting. And, there are ten techniques in which attackers can perform in order to achieve this tactic, and those techniques are active scanning, gather victim host information, gather victim identity information, gather victim network information, gather victim organization information, phishing for information, search closed sources, search open technical databases, search open websites or domains, and search victim-owned websites (MITRE ATT&CK, 2021). Therefore, the attackers can use these techniques to achieve their reconnaissance tactic. Furthermore, for resource development, it contains techniques that attackers can create, buy, or steal resources that can be used to support their target. Within this tactic, there are seven techniques in which attackers can perform in order to achieve this tactic, and they are acquiring infrastructure, compromising accounts,

Proceedings DOI: 10.21467/proceedings.174
ISBN: 978-81-984081-6-7

Series: AIJR Proceedings
ISSN: 2582-3922

compromising infrastructure, developing capabilities, establishing accounts, obtaining capabilities, and staging capabilities (MITRE ATT&CK, 2021). So, these techniques can be used by the adversaries to enhance their resources. Regarding the Windows matrix, all common tactics, techniques, and procedures are clearly discussed and explained. According to MITRE ATT&CK (2021), there are twelve tactics that can be used by attackers to exploit all machines that run Windows as their operating systems. Those twelve tactics are initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact.

First, it is about the initial access. This tactic contains techniques that attackers can use many different points to get their initial access within a target network. Within this tactic, there are many techniques that attackers can do in order to achieve the initial access such as drive-by compromise, exploit-public facing application, external remote service, hardware additions, phishing, replication through removable media, supply chain compromise, trusted relationship, and valid accounts (MITRE ATT&CK, 2021). After that, it is about the execution. This tactic contains techniques that result in attacker-controlled code running on a local or remote target system. In this tactic, attackers can perform many techniques to complete this tactic such as command and scripting interpreter, exploitation for client execution, inter-process communication, native API, scheduled task or job, shared modules, software deployment tools, system services, user execution, and Windows management instrumentation (MITRE ATT&CK, 2021).

Moreover, persistence contains techniques that attackers can utilize in order to keep or remain access to target systems for long-term. Attackers can use many techniques to make this tactic done such as account manipulation, browser extensions, compromise client software binary, create an account, create or modify system process, event triggered execution, external remote service, traffic signaling, and so on (MITRE ATT&CK, 2021). Furthermore, privilege escalation contains techniques that attackers can utilize in order to gain higher-level permissions on a system or network, which involves both horizontal privilege escalation and vertical privilege escalation. There are many techniques that attackers can do in order to achieve this tactic. Those techniques are abuse elevation control mechanism, access token manipulation, boot or logon auto start execution, boot or logon initialization scripts, create or modify system process, domain policy configuration, process injection, and so on (MITRE ATT&CK, 2021).

Regarding the defense evasion, it contains techniques that attackers can utilize in order to avoid being detected with their track. There are many techniques that attackers can do to complete this goal and they are access token manipulation, direct volume access, domain policy configuration, exploitation for defense evasion, file and directory permissions modification, hide artifacts, hijack execution flow, modify registry, rootkit, XSL script processing, and so on (MITRE ATT&CK, 2021). In addition, credential access contains techniques that attackers can utilize in order to steal or dump credentials like usernames and passwords. There are many techniques that attackers can do to achieve this goal and they are adversary-in-the-middle, brute force, credentials from password stores, exploitation for credential access, forced authentication, input capture, modify authentication process, network sniffing, OS credential dumping, steal web session cookie, two-factor authentication interception, unsecured credentials, and so on (MITRE ATT&CK, 2021). What is more, in the discovery tactics, it contains techniques that attackers can utilize to gain more information about their target system, environment, and network. There are many techniques that attackers can do to complete this goal and they are account discovery, application window discovery, browser bookmark discovery, domain trust discovery, file and directory discovery, group policy discovery, network service scanning, network share discovery, network sniffing, password policy discovery, process discovery, query registry, remote system discovery, and so on (MITRE ATT&CK, 2021). Last but not least, lateral movement contains techniques that attackers can utilize in order to exploit their target systems on a particular network. There are many techniques that attackers can do to achieve this tactic and they are exploitation of remote services, lateral tool transfer, remote service session hijacking, remote service, software deployment tools, and so on (MITRE ATT&CK, 2021).

Besides that, collection is also a tactics that contains techniques that attackers can utilize in order to collect information based on the attackers' goals. There are many techniques that attackers can do to achieve this tactic and they are adversary-in-the-middle, archive collected data, audio capture, automated collection, clipboard data, data from local system, data from network shared drive, data from removable media, email collection, input capture, screen capture, video capture, and so on (MITRE ATT&CK, 2021). For command and control tactic, it contains techniques that attackers can utilize in order to talk or communicate with their target systems under their control within a victim network. There are many techniques that attackers can do to achieve this tactic such as application layer protocol, communication through removable media, data encoding, data obfuscation, encrypted channel, non-standard port, proxy, remote access software, web service, and so on (MITRE ATT&CK, 2021).

Also, another tactic is exfiltration, and this tactic contains techniques that attackers can utilize in order to steal or exfiltrate data and information from their target systems or networks. There are many techniques that attackers can do to achieve this tactic as well such as automated exfiltration, data transfer size limits, exfiltration over C2 channel, exfiltration over other network medium, exfiltration over physical medium, exfiltration over web service, and so on (MITRE ATT&CK, 2021). Finally, it is about the impact, and it contains techniques that

attackers can utilize in order to disrupt availability or compromise integrity by making some changes in business and operational processes. There are many techniques that attackers can do to achieve this tactic such as account access removal, data destruction, data encrypted for impact, data manipulation, defacement, endpoint denial of service, firmware corruption, service stop, system shutdown or reboot and so on (MITRE ATT&CK, 2021). Therefore, the attackers can leverage these twelve tactics with its corresponding techniques in each tactic to compromise Windows machines.

5 Cyber Kill Chain and MITRE ATT&CK framework analysis

By taking both Cyber Kill Chain and MITRE ATT&CK framework into analysis, the cyber kill chain model can be considered as an attack methodology which describes all important phases such as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective phase. These phases are the basis of attack methods that attackers need to perform in order to exploit their targets as well as be successful in conducting a cyber-attack. Not only does this model benefit the attackers, it also acts as a great source of knowledge for defenders or information security analysts to know and understand about stages that the attackers will follow in order to compromise their target. Therefore, the defenders can utilize this knowledge to protect and prevent their valuable and critical assets from being exploited by hackers or cyber-criminals. Moreover, this model allows the defenders to track the progress of the attack that targets their organization because it lets the defenders know what phase of the cyber kill chain that the attackers try to achieve and how many phases that the attackers have already exploited. For instance, if cybersecurity analysts detect a lot of suspicious emails within their organization or they are reported about unusual emails by their users, they can immediately investigate and understand that the attackers might be running a phishing campaign or sending payloads to exploit their users and organization. With this information, the cybersecurity analysts can quickly take appropriate actions to defend their organization as well as their users from the attack by breaking the chain of the attack which is the delivery phase for this case. Therefore, the attackers cannot proceed to the next phase of the cyber kill chain after the delivery phase and accomplish their goals.

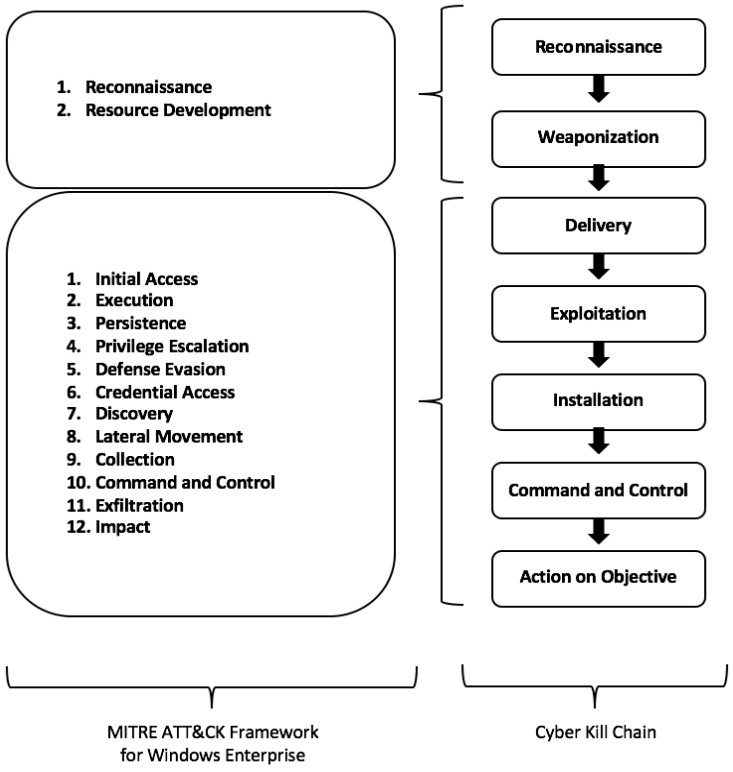

Figure 2: The Relationship between MITRE ATT&CK Framework and Cyber Kill Chain

In spite of that, MITRE ATT&CK framework acts as a book that consists of tactics, techniques, and procedures (TTPs) that the attackers can use to fulfill their goals and objectives in each phase of the Cyber Kill Chain model. As shown in Figure 2, in the first phase of Cyber Kill Chain which is the reconnaissance phase, in order to gather critical information about a target system or environment, the attackers may implement possible

Proceedings DOI: 10.21467/proceedings.174
ISBN: 978-81-984081-6-7

Series: AIJR Proceedings
ISSN: 2582-3922

techniques under reconnaissance tactic in MITRE ATT&CK framework such as performing the active scanning or passive scanning by using "Nmap" or other tools in order to scan their target systems or networks to obtain available and valuable information on the target networks such as sensitive open ports or services which can be considered as loopholes or vulnerabilities presented on the target networks or systems. With this sensitive information, the attackers can invent or build a specific malware or tool based on the techniques and procedures listed in the resource development tactic of the MITRE ATT&CK framework in order to compromise their target, and this is corresponding to the second phase of the cyber kill chain model which is the weaponization phase, and the resource development tactic of the MITRE ATT&CK framework. In addition, for delivery, exploitation, installation, command and control, and action on objective phase of Cyber Kill Chain model can be made by following all techniques and procedures listed in all the tactics of MITRE ATT&CK framework which are from initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact respectively. So, all the tactics, techniques, and procedures of MITRE ATT&CK framework can be used to support all phases of Cyber Kill Chain model.

Therefore, both Cyber Kill Chain and MITRE ATT&CK framework act as complementary models to each other because Cyber Kill Chain model illustrates an attack methodology while MITRE ATT&CK framework provides rich details in term of tactics, techniques, and procedures (TTPs) that can benefit both the attackers and defenders in exploiting target networks or systems as well as protecting critical assets from being compromised.

6 Conclusion

This paper aims at exploring and analyzing the relationship between Cyber Kill Chain and MITRE ATT&CK framework by detailing all the phases of Cyber Kill Chain model with the technical flow from the mindset of the attackers, discussing all tactics and techniques of MITRE ATT&CK framework in the area of preparatory and Windows matrix in the enterprise, and showing on how to leverage the TTPs in MITRE ATT&CK framework and use them in the Cyber Kill Chain model. By doing these, the defenders can understand the attackers' mindset and perspective, especially their attack methodology and its TTPs used in each phase of the attack methodology in a smart way so that they can protect and prevent valuable and critical digital assets from being exploited and compromised by the cyber-criminals. In the future, the scope of this research paper will be expanded because I will take advantages of the relationship between Cyber Kill Chain and MITRE ATT&CK framework to identity particular advanced persistent threat (APT) groups, and how to prevent and protect digital assets from their exploitation.

7 Declarations

7.1 Competing Interests

I would like to declare that I have no conflicts of interest to disclose.

7.2 Publisher's Note

AIJR remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

How to Cite

Phyrum Rithchea (2025). Cyber Kill Chain and MITRE ATT&CK Framework Analysis. *AIJR Proceedings*, 24-29. https://doi.org/10.21467/proceedings.174.5

References

Al-Shaer, R., Spring, J. M, & Christou, E. (2020). Learning the Associations of MITRE ATT&CK Adversarial Techniques. *arXiv*. Retrieved from: https://arxiv.org/abs/2005.01654

Lockheed Martin Corporation. (2015). GAINING THE ADVANTAGE: Applying Cyber Kill Chain Methodology to Network Defense. *LOCKHEED MARTIN*. Retrieved from: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

MITRE. (2021). *MITRE ATT&CK* [Online]. Retrieved from: https://attack.mitre.org/ (visited on February 27th, 2022).

Tarnowski, I. (2017). How to use cyber kill chain model to build cybersecurity?. *European Journal of Higher Education IT*. Retrieved from: https://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf

Yadav, T., & Mallari, R. A. (2016). Technical Aspects of Cyber Kill Chain. *arXiv*. Retrieved from: https://arxiv.org/abs/1606.03184v1