International Journal of Contemporary Research In Multidisciplinary

Review Paper

Unweaving the Cyber Attack - The Cyber Kill Chain Analysis

Ranjan Banerjee[1*], Debmalya Mukherjee[2], Partha Shankar Nayak[3]
Shuvrajit Nath[4], Most Mahabuba Islam[5]

[1,3,4,5]Assistant Professor, Department of Computer Science Engineering, Brainware University, West Bengal, India
[2]Assistant Professor, Department of Computational Sciences, Brainware University, West Bengal, India

Corresponding Author: *Ranjan Banerje

DOI: https://doi.org/10.5281/zenodo.12179781

Abstract

The path followed by an intruder to penetrate information systems over time to develop incident response and analyze capabilities to execute an attack on the victim can be described by a Cyber Kill Chain model, resulting in remarkable disruptive effects on organizations. It is an intrusion-centric model that was the base of cyber security and has been widely used by the security community to describe the different stages of cyber-attacks. Still, for pro-active network defense, early detection of cyber threats is critical to protect against data, financial, and reputation loss that large-scale security breaches could cause. Cyber threat hunting activities are time-consuming, and in-depth analysis and continuous monitoring of related systems and network events are required to achieve the objective, thus becoming critical for inside-out security.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 13-05-2024
- **Accepted:** 14-06-2024
- **Published:** 19-06-2024
- **IJCRM:**3(3); 2024: 114-116

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Manuscript

Ranjan Banerjee, Debmalya Mukherjee, Partha Shankar Nayak, Shuvrajit Nath, Most Mahabuba Islam. Unweaving the Cyber Attack - The Cyber Kill Chain Analysis. International Journal of Contemporary Research in Multidisciplinary.2024; 3(3): 114-116.

KEYWORDS: Network Security, malicious intruders, Data Security, Cyber-attack, Denial of Service, Kill chain, Threat model.

INTRODUCTION

Cyber Kill Chain: An Introduction

With the technological advancement and evolution of sophisticated tools to satisfy cybercriminals' goals, traditional conventional network defense tools such as firewalls and antivirus software approaches, which use static knowledge of existing systems to detect threats and vulnerabilities, are no longer sufficient. Using threat modeling and attack scenarios, along with knowledge of opponents, can significantly reduce the probability of each attempted attack. This approach lets us stop more successful computer attacks, which result in spectacular data leaks [1][2]. It is necessary to analyze and gather information related to the attack process at every stage to understand how a computer attack is launched. A chain of events executed successfully leads to a successful and effective attack beginning from the initial identification phase aiming to know the victim and gather valuable information through hacking. These events can, therefore, be analyzed to gain knowledge and utilize it to break this chain as early as possible to minimize. Not only the weak elements of the system or the system as one entity should be considered for defense, but defending itself against known and unknown threats in a comprehensive manner, independent of the system's weakness, must be considered [3].

Role of System Administrators and Analysts in Cyber-kill Chain

The cyber attackers' main intention is to threaten confidentiality, integrity, and availability and generate authentication and non-repudiation problems by collecting confidential and private data, disrupting services, and denying access to resources. They will always try to find methods to destroy or damage a government, political system or religion or computer network of companies by attacking indirectly without exposing or revealing their identity. The problem gets even more severe in a busy network where the network traffic per day could be massive, so, as a result, the end systems and network devices generate such a large volume of log data that it becomes critical for security analysts and system administrators to detect a potential threat by reviewing and considering every data record in the log and correlate those events at system and network level [4][5]. To make the analyst's life easier, security solutions such as the Security Information and Event Management (SIEM) tool help by collecting the events from various systems and network devices into one place, thereby grouping them into categories and providing easy and centralized access interface to the alerts or logs by delivering an interactive dashboard to help analysts to correlate series of system and network events to determine whether they indicate a potential security breach.

For better understanding and efficient output, the analysts should have a clear concept of cyber threat hunting skills and related experience to discover connections between seemingly unrelated events to be able to spot malicious activities that may have been observed in the network and could be part of a cyber-kill chain with high-impact security breaches having adverse effects [6].

Therefore, the task of the analyst is to try and find out the intention behind the attack, which can be identified by discovering the footprints left behind by the attacker on systems all over the network and tracing network traffic to know which service is being targeted and where the attacker is heading at different instances of time. Detection of threats earlier in the kill chain is essential to prevent data, financial, and reputation loss caused by large-scale security by successfully defending the network. For the computer incident response team to identify participants in the anti-organization more efficiently and to understand the purpose and methods of attack, the help of the kill chain model can be taken so that the directions and methods of defense can be determined, which also requires to build a model based on threat information focusing not only on vulnerabilities but also on threats [7].

Developed by Lockheed Martin as a security framework for incident detection and response, the term *Kill Chain* and the names of the chain phases are derived from military terminologies. In Cybersecurity, the Kill chain may be explained as the stages of an information system attack. The General Cyber Interference Kill Chain is comprised of the following steps:

- **Reconnaissance:** In this stage, the attacker collects data about the target and conducts research on the targeted system's architecture, capabilities, vulnerabilities, etc.
- **Weaponization:** Here, the attacker makes a malicious and exploited payload to ship off the objective by preparing the attack tools and placing them in infected files that the victim will use after delivery—the attackers' code up deliverable payloads [8].
- **Delivery:** The attacker "attack tools" to the attacked environment, i.e., sends the malevolent payload to the target through a pre-prepared attack vector like email or other methods. In other words, the adversaries employ various strategies to send weaponized payloads.
- **Exploitation:** In one sentence, the exploit is executed. The vulnerabilities of the system(s) were exploited, i.e., the code is executed in the attacked environment after delivering the "attack tools" to the victim machine.
- **Installation:** In this stage, Malware, Trojan horses, or so-called " backdoors " are installed in the target system(s). The attacker then installs his or her system in the target system.
- **Command and Control:** Remote control of the infected target device by establishing a hidden channel is gained with compromised entities within the victim system to expand the attack campaign further.
- **Actions on Objective:** The attacker performs malicious activities or executes additional attacks on other devices from within the network. At this point, the right action is taken to achieve the objectives by working through the kill chain stages again.

Network security defenses are designed to defend against the kill chain. A conceptually clear understanding of the stages of the kill chain is essential to putting defensive obstacles in place, slowing down the network, and ultimately preventing the loss of data [9].

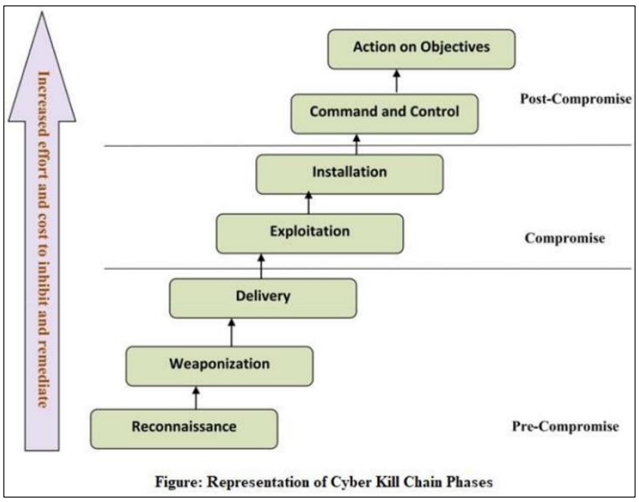

Figure: Representation of Cyber Kill Chain Phases

Cyber Drills

At all levels in the organization, the following are enabled by Cyber drills to improve:

- Information & Cybersecurity Decision-making capability in Information & Cybersecurity scenarios.
- Organizational IT security strategy.
- Response to security incidents

To prevent a cyber-attack, all possible steps should be undertaken by an organization, which could include the best

possible technologies with process controls; an attack may still be successful, but it always prepares to face and encounter such events. With improved technologies and advancements, organizations become increasingly connected, and their risk for cyber breaches shrouds the risk of other cost-related events like natural disasters and fires. Additionally, executives and leaders ultimately held accountable for protecting their organization's data face increased personal risk (remember Uber and Equifax?). Most organizations need to strengthen their reactive controls and mainly concentrate only on preventive and detective controls. Most business continuity and disaster recovery plans do not consider cyber security risks or resilience plans, and organizations need to evaluate if their staff is capable and trained to respond to cyber incidents. Organizations should initiate periodic evaluations to check their cyber incident response capabilities, which can happen through mock cyberwar drills or simulation exercises. [10] [11]

For the defender team to determine the actions to be taken, the phases of cyber-attack should be analyzed and the attack may be detected which may take different character and it's not that it's going to take place very early in terms of model phases; instead, such a detection can occur in each phase of the attack beginning from the reconnaissance phase. The implementation in the action phase illustrates that the attacker's target has the most devastating impact on the organization on which the attack is launched. The moment of detection and recognition of the attack decides the steps to be taken by incident response teams [12].

How can a Cyber Kill Chain be used in security?

A cyber kill chain can be used to find security gaps within seconds. Cyber kill chain can protect against cyber security attacks:

1. Imitation Cyber Security Attacks

Original cyber security attacks can be imitations all over the vectors to find weaknesses and warnings. This includes imitation cyber-attacks through email, websites, web applications, and more.

2. Examine the Controls

In this step, evaluate the assumption and search for factors of risk. These platforms give you a detailed risk score and report on every vector.

3. Fix the Cyber Security Gaps

In these steps, patches are installed and configurations are slightly changed to reduce the number of threats and vulnerabilities in the organization's system.

CONCLUSION

To create efficient detection plans to achieve the full benefit, a conceptually clear understanding of each data log's format and security context is necessary, and it is essential to pay attention and establish some initial foundations. However, challenges still come from all corners within its systems and outside. Also, let's remember that attackers are equipped with Machine Learning powers, and systems can be built to predict the behaviors of the defending models.

REFERENCES

1. Barnum S. An Introduction to Attack Patterns as a Software Assurance Knowledge Resource. In: OMG Software Assurance Workshop; 2007 Mar; Fairfax, VA.
2. MACCDC. Capture files from Mid-Atlantic CCDC (Collegiate Cyber Defense Competition). Available from: https://www.netresec.com/?page=MACCDC. Accessed: 2024-06-19.
3. Hu D, Hong P, Chen Y. FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference. IEEE; 2017 Dec. pp. 1-7. Available from: http://ieeexplore.ieee.org/document/8254023/.
4. Blowers M, Williams J. Machine Learning Applied to Cyber Operations. Springer New York; 2014. pp. 155-175. Available from: https://goo.gl/b0f0tu.
5. Tulabandhula T, Rudin C. Machine Learning with Operational Costs. J Mach Learn Res. 2013;14:1989-2028. Available from: http://www.jmlr.org/papers/volume14/tulabandhula13a/tulabandhula13a.pdf.
6. Apache Organization. Apache Spot. Available from: http://spot.incubator.apache.org/.
7. Microsoft. Microsoft Security Development Lifecycle. Available from: https://www.microsoft.com/en-us/SDL/process/implementation.aspx.
8. Buczak AL, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Commun Surveys Tuts. 2016;18(2):1153-1176. Available from: http://ieeexplore.ieee.org/document/7307098/.
9. Liu W-X, Zhang J, Liang Z-W, Peng L-X, Cai J. Content Popularity Prediction and Caching for ICN: A Deep Learning Approach With SDN. IEEE Access. 2018;6:5075-5089.
10. Internet Engineering Task Force. RFC 1459: Internet Relay Chat Protocol. Available from: https://tools.ietf.org/html/rfc1459.
11. Varonis. Cyber Kill Chain. Available from: https://www.varonis.com/blog/cyber-kill-chain/.
12. Wikipedia. Kill chain. Available from: https://en.wikipedia.org/wiki/Kill_chain.