fn Cyber
CyberSecurity Simplified

CYBER KILL CHAIN

A COMPREHENSIVE OVERVIEW

Have you ever thought about how cybercriminals carry out their attacks? The Cyber Kill Chain model, developed by Lockheed Martin, breaks down their strategies into seven easy-to-understand stages. From the initial steps of gathering information to the final stage of stealing data, this model helps organizations grasp the entire attack process. It's like a roadmap that shows us how cyberattacks happen. By using this model, companies can better prepare and defend themselves against cyber threats. It's not just about reacting when an attack occurs; it's about being proactive in preventing them. By understanding the motives behind cyberattacks, we can develop stronger defenses. In today's digital world, where cybersecurity is crucial, embracing the Cyber Kill Chain model can make a significant difference in keeping our information safe.

The seven phases of Cyber Kill Chain are:

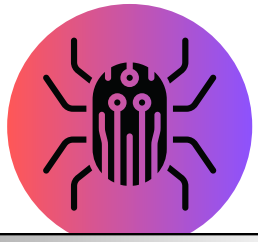
1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control
7. Actions on Objectives

fn Cyber
CyberSecurity Simplified

7 Steps of Cyber Kill Chain

1

Reconnaissance

2

Weaponization

3

Delivery

4

Exploitation

5

Installation

6

Command & Control

7

Actions on Objectives

fn Cyber
CyberSecurity Simplified

The Initial Phase: Reconnaissance

In the first phase of the Cyber Kill Chain, malicious actors engage in reconnaissance. They gather information about the target, laying the groundwork for a successful attack. During this phase, attackers identify vulnerabilities in systems, find valuable data, and craft their strategies accordingly.

1 Information Gathering

Attackers collect data on target personnel, networks, and systems through various means like social media, phishing emails, and network scans.

2 Identifying Vulnerabilities

By probing for weaknesses, cyber criminals pinpoint exploitable features within the system's defenses they plan to breach.

3 Strategic Planning

Tailoring their attack to the gathered intelligence ensures a higher chance of success when they move forward with the intrusion.

fn Cyber
CyberSecurity Simplified

Weaponization: Crafting the Attack

Once sufficient information has been gathered, adversaries enter the weaponization phase. They develop the malicious payload that will allow them to exploit the identified vulnerabilities, often involving the creation of malware tailor-made to infiltrate the specific target.

1 Malware Creation

Malicious software is coded, often designed to ensure stealth and effectiveness in targeting the victim's infrastructure.

2 Matching Exploits

Attackers choose exploits that correspond with the vulnerabilities discovered during reconnaissance.

3 Payload Integration

The exploit is packaged with the payload, such as a virus or worm, ready to be delivered to the target.

fn Cyber
CyberSecurity Simplified

Delivery: The Attack Commences

With the weaponized payload ready, attackers proceed to the delivery stage, where they deploy the malicious payload to the victim's environment. This critical phase determines whether the planned attack will gain a foothold within the target's network.

1. Email Phishing

Attackers often send emails with infected attachments or links. Once opened or clicked, the payload is executed.

2. Exploiting Public-Facing Applications

Cybercriminals can also leverage vulnerabilities in web applications to deliver their payload passively.

3. USB & Removable Media

Infected devices, when plugged into the network, can serve as another delivery vector for the attack.

fn Cyber
CyberSecurity Simplified

Exploitation: The Breach Is Executed

Successfully delivering the payload allows attackers to move on to exploitation. In this phase, the payload is activated, and system vulnerabilities are leveraged to gain unauthorized access to systems and data.

1.Exploit Execution	The payload, often malicious code, is executed to take advantage of system vulnerabilities.
2. Access Methods	Can include buffer overflow, SQL injection, or use of stolen credentials.
3. Immediate Impact	Varying from minor disruptions to complete system takeovers.

fn Cyber
CyberSecurity Simplified

Installation: Ensuring Persistence

Following a successful exploitation, attackers aim to establish a persistent presence within the target network. Installation phase encompasses the tactics used to maintain control over compromised systems, even as they work to evade detection.

1 Backdoors	2 Rootkits	3 C&C Channels
Attackers install backdoors to ensure future access, bypassing normal authentication procedures.	By deploying rootkits, adversaries gain deeper control and can hide their activities from system administrators.	Command and control (C&C) channels are set up for communication with compromised systems to issue commands remotely.

fn Cyber
CyberSecurity Simplified

Command and Control: Remote Manipulation

With persistent access established, attackers shift to commanding the compromised systems remotely, steering the attack using the infrastructure they've implemented. The Command and Control phase is when the real damage can begin if left unchecked.

1. **C&C Servers** → The centralized points that direct compromised systems, often hidden in normal network traffic.

2. **Malware Communication** → The method by which installed malware communicates and receives commands from the attackers.

3. **Remote Execution** → Attackers remotely control systems, execute commands, and move laterally within the network.

fn Cyber
CyberSecurity Simplified

Actions on Objectives: The Endgame

Having established control over the network, attackers execute their ultimate objectives. Depending on the motivation, this may involve data theft, system damage, or setting the stage for a more significant, long-term exploitation operation.

1

Data Exfiltration

Stealing sensitive data is often the goal, which can include personal information, trade secrets, or financial records.

2

Destruction

Some attacks aim to incapacitate systems, destroy data, or disrupt operations.

3

Resource Exploitation

Accessed systems may be used for further attacks, to host illicit content, or mine cryptocurrency.

fn Cyber

CyberSecurity Simplified

fnCyber was incepted with the sole purpose of uncovering vulnerabilities in any business system at the functional level, combining the expertise in Business Continuity, Cybersecurity and Integrated Risk Management, taking the Cybersecurity Practice to organizational grassroots and infusing IT Security Controls with procedural awareness transforming enterprises as they go Cyber Resilient - Functionally.

Our team of cybersecurity experts has a wealth of knowledge when it comes to identifying and reducing cyber risks for businesses.

To learn more, visit us at

www.fncyber.com

info@fncyber.com