CYBER KILL CHAIN BY P3NGU1N

INTRODUCTION TO CYBER KILL CHAIN

What is Cyber Kill Chain?

- **is a framework**
- **created by Lockheed Martin in 2011 (was established in 1995 and it is a security and aerospace corporation)**
- it contains attacker behavior
- through what steps or stages it goes through to carry out a cyber attack

why important for SOC Analyst?

- to better understand attackers tactics
- determine the severity of security flaws
- threat hunting is easier by understanding attackers tactics

🎯 QUESTION :

Which organization was the Cyber Kill Chain model developed by?

ANSWER: lockheed martin

🎯 QUESTION :

In what year was the organization that developed the Cyber Kill Chain model founded?

ANSWER: 1995

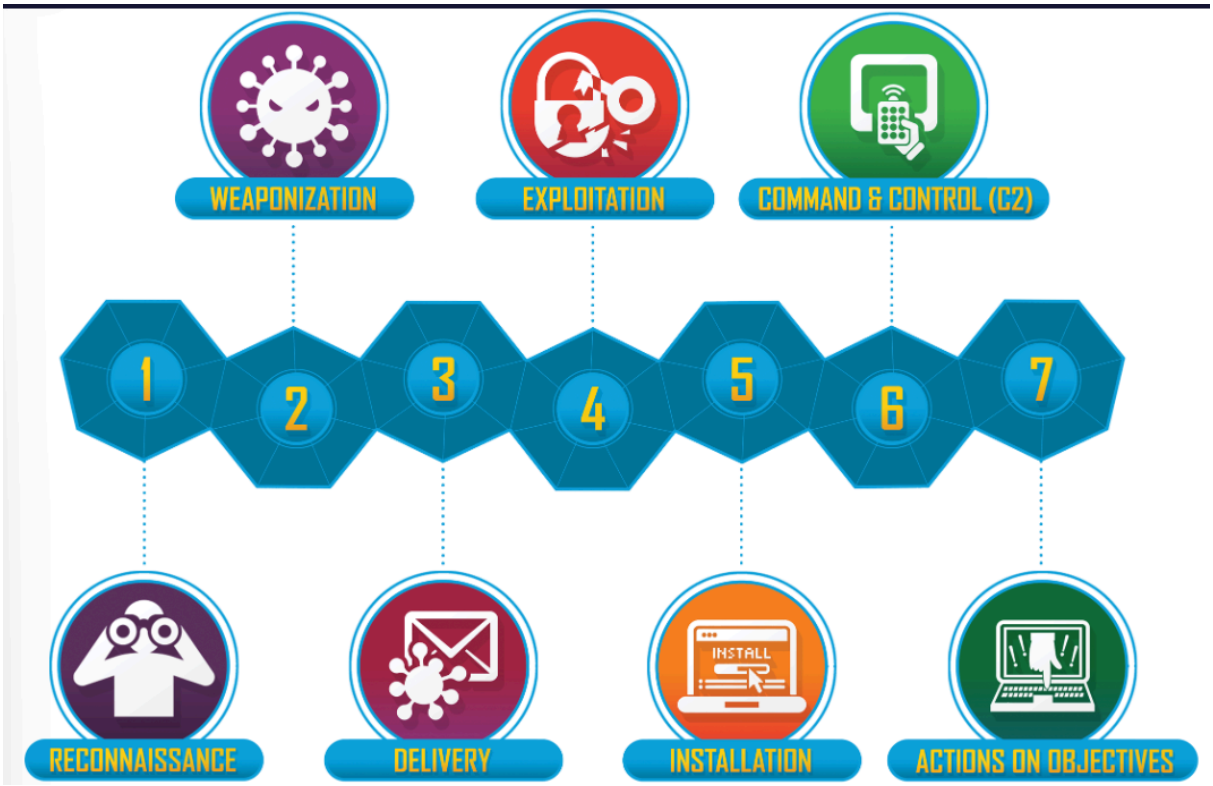
🎯 QUESTION :

In what year was the Cyber Kill Chain model developed?

ANSWER: 2011

Cyber Kill Chain Steps

- 7 STEPS
- work like a chain
- 2nd works only if previous step is completed



🎯 QUESTION :

How many steps does the Cyber Kill Chain model consist of?

ANSWER: 7

Reconnaissance:

- first step
- obtains info
- more info, greater attack surface
- Attack vectors for the target are disclosed in this way.

The techniques employed at this stage may be divided into two subcategories:

- Passive Reconnaissance → without physical engagement
- Active Reconnaissance → by engaging with it directly

Adversaries:

attacker can perform the following actions:

- version info of servers
- ip block of organization
- employee mail
- employee whereabouts from social media
- info from open source previously released
- devices using internet
- what third party organizations they are in contract with

Defender:

- how can attacker strategies be taken down at this stage in CKC:
- monitor traffic
- security solutions like firewall, IDS, IPS
- update for patching new vulnerabilities
- keep minimal information on the internet
- obtain leak info through threat intelligence and remove it

🎯 QUESTION:

What is the step in the Cyber Kill Chain model where the information gathering takes place?

ANSWER: Reconnaissance

APT Group:

Lazarus Group-APT38

Year of Cyber Attack Detection: 2019

Real-life Attack Scenario:

- The APT38 group has targeted an institution in the financial sector for a cyber attack.
- Information was collected by conducting reconnaissance operations for several days on the organization’s website determined as the target of the cyber attack.
- A security vulnerability with the code "CVE-2019-0604" has been found in the organization's use of Microsoft SharePoint product.
- The identified security vulnerability was exploited.
- After the successful exploit, the "Powershell Empire" backdoor was deployed to the target system.

🎯 Question:

The Real-life attack Scenario items above explain an aspect of an actual cyber attack. Based solely on this information, what is the number of distinct actions taken during the "Reconnaissance" phase, which is the first step of the Cyber Kill Chain?

Note:

Consider each sentence in the list as a separate action. The scenario's actions are all consecutive. Enter the answer as a numerical value.

ANSWER: 3(1. targeting financial sector , 2. info collected by site, 3. vulnerability was found)

Weaponization

- second step in the Cyber Kill Chain.
- information obtained in the previous stage to access the tools needed for the attack
- or makes a new script
- If the tools for the cyber attack are ready, the attacker completes this phase
- victim is generally unaware of the attacker.

Adversary

- malware creation
- exploit scripts
- phishing content, malicious email content
- finding best tool to perform attack

Defender:

some measures can be taken:

- **see if any identified security vulnerabilities exist.**
- install security updates
- analyze impacts of new threats

Attack Scenario:

- An APT group selected a telecom organization as the target of a cyber attack.
- E-mail addresses of the selected organization were collected through social media and open sources.
- A phishing e-mail template was generated to be sent to the e-mail addresses of the organization's employees based on the information obtained.
- A Word document titled "Salaries.docx" containing malicious macro code was created to be included in the email attachment.
- The prepared phishing e-mail was sent to the victim e-mail accounts on the specified date.
- The e-mail was viewed by some employees of the organization and the malicious Word document was downloaded.
- The malicious Word document that the victim had downloaded was opened, and the macro code contained therein was run.
- The ransomware was installed and ran on the victim's device using malicious powershell code in the macro code.

🎯 **Question:**

How many separate activities were performed in the "Weaponization" phase, the second step of the Cyber Kill Chain, according to the Attack Scenario items above?

Note:

Consider each statement in the scenario as a separate action. The scenario's actions are all consecutive. Enter the answer as a numerical value.

ANSWER: 2(1. email template generation, 2. .docx with malicious macros)

DELIVERY

- 3rd step
- attacker executes the attack
- interaction with victim
- malicious content is uploaded to an environment
- victim is made to download that content means delivery of malicious content is done

Adversary:

attacker can deliver various cyber weapons

- malicious url via mail
- malware as file via mail
- via usb
- url via social media
- malware via social media

- directly into server if access
- make him download via a website

Defender:

blueteam can take plenty of precautions at this stage

- URL in sandbox first
- scanning email files using antivirus first
- email security products
- banning physical malicious content transfer by panning usbs
- use and management of firewall
- log management is very important at this stage
- constant monitoring
- proper training of employees regarding information security and attack prevention startegies

Attack Scenario:

- An APT group targeted a defense sector institution with a cyber attack.
- The IP addresses of the selected organization were detected via Shodan and Zoomeye.
- According to the information obtained from open sources, it was learned that the organization uses the Windows operating system.
- Malware was embedded in "putty.exe" a legitimate tool to run on Windows machines in the organization, with the help of the Metasploit tool.
- This malware was transferred to several different USB sticks.
- The USB sticks were left on a nearby sidewalk to the institution used by the employees before work.
- Shortly after starting work, a curious employee plugged the USB stick into a company computer connected to the corporate network.
- He/She executed the program named "putty.exe" on the USB stick.

- After the program was executed, the attacker was able to temporarily execute remote commands on the company computer in the organization via the reverse connection.
- The attacker added a new scheduled task on the Windows machine to ensure persistence.
- The EDR product on Windows marked the added scheduled task as suspicious.
- The SOC analyst noticed an alert named "Suspicious Scheduled Task Detected" on their security monitor.
- After analyzing the alert, the SOC analyst took the necessary actions and prevented the cyber-attack from moving to further stages.

🎯 **Question:**

According to the Attack Scenario items above, how many different actions were performed in the "Delivery" phase, the third step of the Cyber Kill Chain?

ANSWER: 2 (1. malware transferred to usb stick, 2. USB sticks were left on a nearby sidewalk)

🎯 Question:

How many separate activities were performed in the "Weaponization" phase, the second step of the Cyber Kill Chain, according to the Attack Scenario items above?

ANSWER: 2 (1. putty.exe embedded malware, 3. malware transferred to USB)

EXPLOITATION:

- 4th step
- it is ensured that malicious content is to be activated
- running the malware
- next steps of exfiltration etc. cannot be carried out if this fails
- next steps depend on this

Adversary:

- attacker runs the tool it has sent in delivery phase
- if tool fails or malware it has sent fails
- means it could not exploit the system mean its not suitable for the the system it was crafted for
- exploiting software, hardware vulnerability
- running malware

Defender:

- more task for blue team in this phase
- training of employees
- constant monitoring
- scanning files
- security updates
- secure coding in software development
- regular automated vulnerability scanning

INSTALLATION

- fifth phase of the Cyber Kill Chain

- attacker attempts to maintain persistence on the target system
- by installing a backdoor
- Because the exploited vulnerability will be patched
- the malware to be installed on the target device can alternatively be placed with the help of a dropper
- to acquire access to a highly authorized user account
- stage at which attack preparations are carried out to achieve aim

Adversary:

- The attacker can successfully perform various technological activities provided that they are constrained to their authority in the system
- ensure that security products do not interfere with the operations
- install malware
- place backdoor
- install webserver
- scheduling task
- adding a custom firewall rule to make it look legitimate and not sus

Defender:

- blue team apply threat hunting at this stage
- **SOC team should manage and execute security operations under the assumption that there is always an attacker present**
- network monitoring on system
- EDR security to be aware of configuration changes
- restricting access to files and path
- process management
- dont allow files to be run
- detect anomalies and fined root cause

Detection Scenario:

The EDR product detected malware on a machine within the organization. The SOC analyst examined the machine and determined that the malware was not executed and no malicious system activity occurred on the machine.

🎯 **Question:**

According to the above detection scenario, what is the Cyber Kill Chain step where the attacker fails and the attack is detected?

ANSWER: 4

COMMAND & CONTROL (C2)

- 6th step in CKC
- attacker has done most of the attack to stay persistent
- formed a c2 channel/server to send commands to system remotely and execute them

Adversary:

- Attacker does not perform the actual malicious action
- it forms a remote connection to run commands
- check necessary things needed from victims system to be fully prepared to perform final action

Defender:

- general security monitoring and detection techniques
- steps to recognize and prevent potential C2 network traffic flow

- determine whether the known C2 tools are available on systems
- Blocking C2 server IP addresses from Cyber Threat Intelligence sources
- C2 communication with Network Security Monitoring on the system

Detection Scenario:

In its network connections, a Windows machine within the organization appeared to have successfully established a connection to a suspicious IP address outside the organization. With this connection, the SOC analyst determined that the attacker was able to execute remote commands on the Windows machine.

🎯 **Question:**

What is the last Cyber Kill Chain step in which the attacker is successful, according to the aforementioned detection scenario?

ANSWER: 6

ACTIONS ON OBJECTIVES

- 7th and final step
- attacker achieves the goal it started the attack with
- each task before this needed to be completed successfully to be able to reach this stage
- now attacker can carry out desired operation

Adversary:

- **attackers' actions are determined by their purpose and motivation**
- encrypt files
- delete databases

- disrupt other actions
- privilege escalate to expand to other devices in network like a replicating worm
- changing info, harming integrity
- collecting info for some other target
- manipulating info for reputational damage

Defender:

- regular monitoring
- **prevent attackers from exfiltrating data from the organization to outside**
- Detecting anomalies in network
- Restricting network access to the outside
- Restricting access to files/folders containing critical information
- Restricting the authorization of access to databases containing critical information
- Using DLP products to prevent data leakage
- Detecting unauthorized access by users

🎯 QUESTION:

The usage of the "SDelete" tool for data deletion by the APT group "Cobalt Group" is an activity at which stage of the Cyber Kill Chain?

ANSWER: 7

QUIZ

1. **What is the Cyber Kill Chain step in which the ultimate assault targets are executed by the attacker?**

ANSWER: Actions on objectives

2. **At what stage of the Cyber Kill Chain does the attacker create the tools to be used in the attack?**

ANSWER: Weaponization

3. **What is the Cyber Kill Chain phase in which the attacker connects to the target PC and gets ready to transmit commands?**

ANSWER: C2

4. **Which initial stage of the Cyber Kill Chain involves the attacker using privilege escalation to maintain persistence on the victim's device?**

ANSWER: Installation

5. **What is the Cyber Kill Chain step in which the attacker installs malicious content on the victim's system prior to the exploit process?**

ANSWER: Delivery
