Cyber Attack Life Cycle

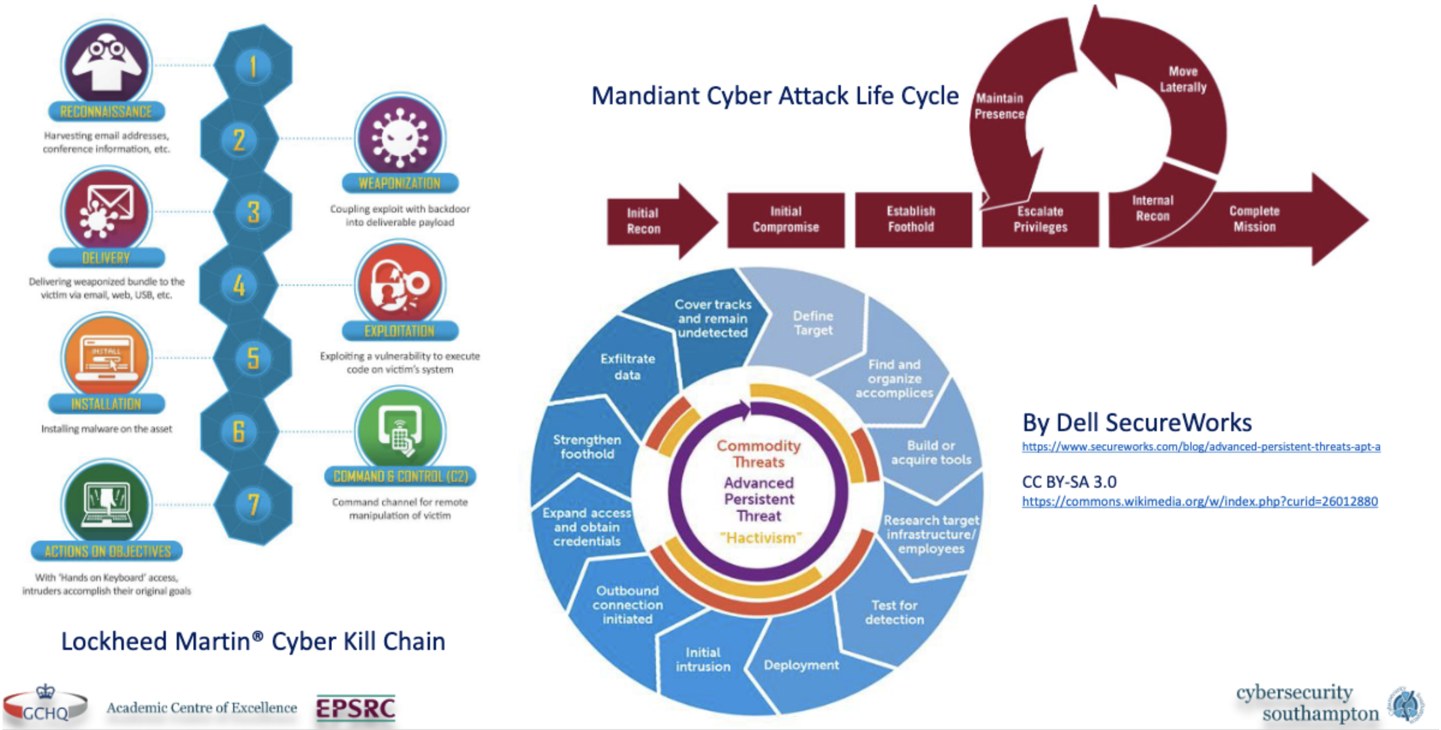
Josh Wilcox (jw14g24)

March 28, 2025

Table of Contents

Cyber Attack Life Cycle Model

- A cyber attack life cycle model is an empirical model representing the sequence of steps that cyber attacks go through



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Lockheed Martin® Cyber Kill Chain

Mandiant Cyber Attack Life Cycle

By Dell SecureWorks
https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

CC BY-SA 3.0
https://commons.wikimedia.org/w/index.php?curid=26012880

GCHQ Academic Centre of Excellence EPSRC

cybersecurity southampton

- They make it easier to understand cyber attacks
- Help to figure out why past attacks have succeeded
- Provide effective ways to protect assets
- Forecast potential next steps of an ongoing attack

Lockheed Martins Keychain Model

2 Lockheed Martins Keychain Model

- Reconnissaince
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Reconnissaince

- Target research and selection
- The **information** the attackers has gathered to plan an attack
- Companies should think about what information makes them a choice, vulnerabilities
- How can attackers access information?
- **Examples:**
  - Crawling of websites to gather email addresses
  - Scans and probes to identify the security means used by the target

Weaponisation

- Development of the required cyber weapons needed to carry out an attack
  - Malware
  - Malicious Payload
  - Exploits
- **Examples**
  - PDF with malicious scripts
  - Stolen Credentials
  - Phishing Emails

Delivery

- The method of actually sending the weapon to the target
- The process of choosing where to send the weapon from
- The decision of where and how to send the method
- **Examples**
    - A malicious link from a website
    - Email Attachments
    - USB stick attacks

Exploitation

2. Lockheed Martins Keychain Model
    - Reconnissaince
    - Weaponisation
    - Delivery
    - Exploitation
    - Installation
    - Command and Control
    - Actions on Objectives
    - Exploitation
    - Installation
    - Command and Control
    - Actions on Objectives

Installation

2 Lockheed Martins Keychain Model

- Reconnissaince
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Command and Control

2 Lockheed Martins Keychain Model

- Reconnissaince
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Actions on Objectives

2. Lockheed Martins Keychain Model
   - Reconnissaince
   - Weaponisation
   - Delivery
   - Exploitation
   - Installation
   - Command and Control
   - Actions on Objectives
   - Exploitation
   - Installation
   - Command and Control
   - Actions on Objectives

Exploitation

- The process of triggering the vulnerability to execute the malicious code
- Exploits system, software, or human vulnerabilities
- Often requires user interaction or system weakness
- **Examples**
  - Buffer overflow attacks
  - Cross-site scripting (XSS)
  - SQL injection
  - Social engineering that tricks users into executing malicious code

Installation

- The process of installing malware on the victim's system
- Creates persistence to maintain access even after system reboots
- May involve installing backdoors or other access mechanisms
- **Examples**
  - Installing rootkits that hide malicious activity
  - Creating new user accounts with elevated privileges
  - Modifying startup processes to ensure malware runs on reboot
  - Hiding malware in legitimate system processes

Command and Control

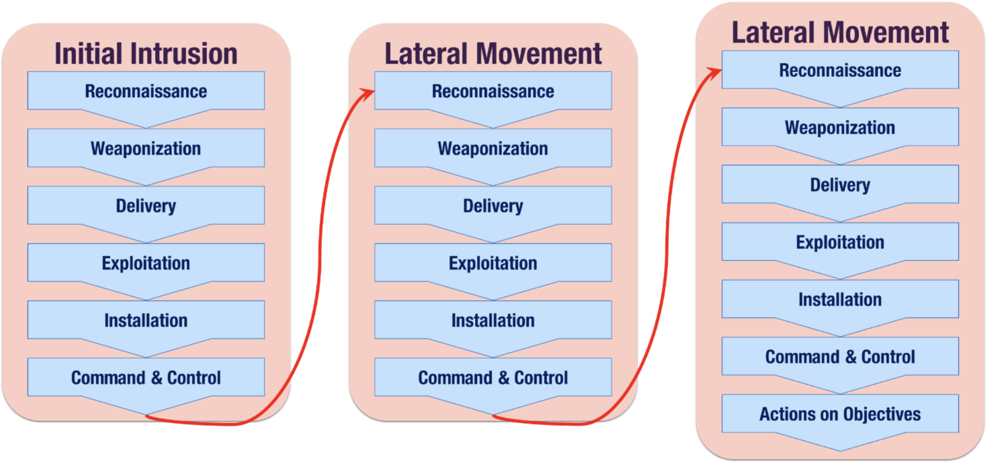
- Establishing a communication channel between attacker and victim
- Allows attackers to remotely control the compromised system
- Often uses encrypted or obfuscated communications to avoid detection
- **Examples**
  - Using HTTP/HTTPS for command communications that blend with normal traffic
  - DNS tunneling to hide command traffic
  - Establishing encrypted communication channels
  - Using legitimate services (like social media) as command channels

Actions on Objectives

- The final stage where attackers achieve their goals
- Can involve data exfiltration, destruction, or manipulation
- The objective depends on the attacker's motivation (financial, espionage, etc.)
- **Examples**
  - Data theft of personal information, intellectual property, or credentials
  - Encrypting files for ransomware attacks
  - Destroying or altering critical data
  - Using the compromised system to attack other targets

Multi-Step Cyber-Attacks

- Complex attacks that involve multiple stages and techniques
- Often executed over extended periods of time
- Require careful planning and execution by sophisticated threat actors
- Usually target high-value organizations or sensitive data
- **Examples**
  - Advanced Persistent Threats (APTs)
  - Supply chain attacks
  - Attacks against critical infrastructure
  - Corporate espionage campaigns
- **The Process**
  1. Attackers scan web for vulnerable servers
  2. They find a vulnerability within the servers
  3. Attackers locate additional servers and credentials
  4. They slowly and quietly extract data to avoid detection



Initial Intrusion

- The first step where attackers establish their foothold in the target environment
- Usually exploits the weakest points in the security perimeter
- Often relies on social engineering or known vulnerabilities
- **Examples**
  - Compromising user credentials through phishing
  - Exploiting unpatched vulnerabilities in internet-facing systems
  - Leveraging infected third-party software or hardware
  - Using watering hole attacks to target specific users

Lateral Movement

- The process of navigating through the internal network after initial access
- Attackers expand their control by compromising additional systems
- Involves privilege escalation and credential harvesting
- Often mimics legitimate administrative activity to avoid detection
- **Examples**
  - Using tools like PsExec, WMI, or PowerShell for remote execution
  - Pass-the-hash and pass-the-ticket attacks to reuse credentials
  - Abusing trust relationships between systems
  - Exploiting internal vulnerabilities not visible from outside

Data Exfiltration

- The extraction of valuable information from the compromised network
- Often happens slowly to avoid triggering security alerts
- Uses encrypted or covert channels to hide the data transfer
- May involve staging data before final extraction
- **Examples**
  - Using encrypted web traffic (HTTPS) to blend with normal communications
  - DNS tunneling to encode data in DNS queries
  - Steganography to hide data within images or other files
  - Exfiltrating data through legitimate cloud services like Dropbox or OneDrive