MITRE ATT&CK FRAMEWORK: A COMPREHENSIVE GUIDE

VAISHALI SHISHODIA

1. Introduction to MITRE ATT&CK Framework

The **MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework** is a globally recognized knowledge base that catalogs real-world cyber adversary behaviors. Developed by **MITRE Corporation**, it helps cybersecurity professionals understand and analyze threats to strengthen their defense strategies.

Why is MITRE ATT&CK Important?

- **Threat Intelligence & Detection**: Helps map attack behaviors to known adversaries.
- **SOC (Security Operations Center) Analysis**: Enables the identification of attack patterns in SIEM alerts.
- **Incident Response**: Guides rapid detection and mitigation.
- **Red & Blue Teaming**: Assists in adversary emulation and threat hunting.
- **Security Policy Improvement**: Strengthens security posture by addressing identified weaknesses.

2. Importance in Detection & Alerting

SOC teams rely on MITRE ATT&CK to **detect cyber threats** based on real-world adversary tactics and techniques. Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) solutions, and Intrusion Detection Systems (IDS) integrate ATT&CK mappings to **generate alerts** based on suspicious activity.

For example:

- **T1566.001 (Spearphishing Attachment)**: If an email with a malicious attachment is detected, an alert is triggered.
- **T1003 (Credential Dumping)**: If an unauthorized LSASS memory dump is detected, an alert is generated.
- **T1046 (Network Service Scanning)**: A sudden increase in port scanning activity triggers an alert.

3. Breakdown of ATT&CK Tactics and Techniques with Real-Life Scenarios

Tactic 1: Initial Access (How attackers gain entry)

- **T1566.001 – Spearphishing Attachment**
    - **Scenario**: An employee receives an email that looks like it's from the HR department, urging them to open an attachment labeled **"Urgent Salary Update.pdf"**. Once opened, a malicious macro runs, installing malware on the system.
    - **Real-life Example**: The **2016 DNC Hack** involved phishing emails that led to malware installation.

Tactic 2: Execution (How attackers execute malicious code)

- **T1204.002 – Malicious File Execution**
    - **Scenario**: A user downloads a pirated software crack from an unverified website. Running the executable installs a backdoor instead of the intended software.
    - **Real-life Example**: Emotet malware spreads through malicious attachments.

Tactic 3: Persistence (Maintaining foothold in the system)

- **T1547.001 – Registry Run Keys/Startup Folder**
    - **Scenario**: Malware modifies Windows registry keys to execute automatically when the system starts, allowing it to persist even after a reboot.
    - **Real-life Example**: TrickBot malware uses registry changes for persistence.

Tactic 4: Privilege Escalation (Gaining higher access)

- **T1068 – Exploiting Vulnerable Services**
    - **Scenario**: An attacker exploits an unpatched Windows vulnerability (e.g., PrintNightmare) to gain administrative access on a compromised machine.
    - **Real-life Example**: EternalBlue exploit was used in WannaCry ransomware for privilege escalation.

Tactic 5: Defense Evasion (Avoiding detection)

- **T1070.004 – Clear Windows Event Logs**
    - **Scenario**: A hacker deletes event logs after gaining access to prevent detection by security analysts.
    - **Real-life Example**: APT groups often clear logs post-compromise to avoid detection.

Tactic 6: Credential Access (Stealing login credentials)

- **T1003.001 – LSASS Memory Dumping**
    - **Scenario**: An attacker uses Mimikatz to extract login credentials from memory to escalate privileges or move laterally.
    - **Real-life Example**: Mimikatz is a popular tool used for credential theft.

Tactic 7: Discovery (Learning about the target environment)

- **T1018 – Remote System Discovery**
    - **Scenario**: Attackers run **"net view"** and **"nslookup"** commands to find other systems and valuable targets on the network.
    - **Real-life Example**: SolarWinds attackers used discovery techniques to move laterally.

Tactic 8: Lateral Movement (Spreading within the network)

- **T1021.002 – SMB/Windows Admin Shares**

- **Scenario**: Attackers use stolen credentials to move from one machine to another using SMB shares.
- **Real-life Example**: Ryuk ransomware used SMB shares to propagate.

Tactic 9: Collection (Gathering sensitive data)

- **T1114.002 – Email Collection via Outlook**
  - **Scenario**: Attackers deploy a tool that silently exports all emails from the victim's Outlook inbox.
  - **Real-life Example**: BEC (Business Email Compromise) attacks target executive emails.

Tactic 10: Command and Control (C2) (Communicating with attacker infrastructure)

- **T1071.001 – Web Protocols**
  - **Scenario**: A trojanized application communicates with an attacker-controlled server over HTTPS to receive commands.
  - **Real-life Example**: Cobalt Strike uses web-based C2 communication.

Tactic 11: Exfiltration (Stealing data from a network)

- **T1567.002 – Cloud Storage Exfiltration**
  - **Scenario**: An attacker scripts an automated process to exfiltrate sensitive files to a Google Drive account.
  - **Real-life Example**: APT29 used Dropbox to exfiltrate stolen government documents.

Tactic 12: Impact (Disrupting operations or causing damage)

- **T1486 – Data Encryption for Impact (Ransomware)**
  - **Scenario**: An organization's critical files are encrypted by ransomware, and the attackers demand payment to restore access.
  - **Real-life Example**: The **Colonial Pipeline ransomware attack (2021)** disrupted fuel supplies.

4. Tools Used by SOC Teams for Investigation and Mitigation

SOC teams rely on various security tools to detect, analyze, and mitigate attacks based on the MITRE ATT&CK framework. Some of the key tools include:

Detection & Monitoring:

- **SIEM (Security Information and Event Management) Tools**: Splunk, IBM QRadar, Elastic SIEM
- **EDR (Endpoint Detection and Response) Solutions**: CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne

- **NDR (Network Detection and Response) Solutions**: Darktrace, Cisco Secure Network Analytics, Vectra AI
- **IDS/IPS (Intrusion Detection/Prevention Systems)**: Snort, Suricata, Zeek (formerly Bro)

Investigation & Threat Intelligence:

- **Threat Intelligence Platforms**: MISP (Malware Information Sharing Platform), Recorded Future, VirusTotal
- **Digital Forensics & Incident Response (DFIR) Tools**: Autopsy, Volatility, FTK (Forensic Toolkit)
- **MITRE ATT&CK Navigator**: Used for mapping techniques to attack behaviors

Mitigation & Response:

- **Endpoint Protection Platforms (EPP)**: Symantec Endpoint Protection, Trend Micro Apex One
- **SOAR (Security Orchestration, Automation, and Response) Tools**: Palo Alto Cortex XSOAR, Splunk Phantom, IBM Resilient
- **Firewall & Web Filtering Solutions**: Palo Alto Firewalls, Cisco Umbrella, Zscaler

These tools enable SOC teams to **detect, investigate, and respond** to cyber threats efficiently, leveraging MITRE ATT&CK to enhance threat-hunting capabilities.

5. Real-Life Story: How a SOC Team Used MITRE ATT&CK to Stop a Cyber Attack

The Incident: A Suspicious Email

One morning, an employee at a financial firm received an email with the subject: **"Urgent: Payroll Discrepancy"**. The email, appearing to be from HR, contained an Excel attachment titled **"Salary_Adjustments.xlsx"**. The employee, believing it to be genuine, opened the file and enabled macros.

Phase 1: Initial Access (T1566.001 – Spearphishing Attachment)

The SOC team's **SIEM (Splunk)** flagged an anomaly: the employee's system made an unusual outbound connection to an external IP. Using **MITRE ATT&CK**, the SOC team mapped this behavior to **Initial Access tactics** and started investigating.

Phase 2: Execution (T1204.002 – Malicious File Execution)

The team used **CrowdStrike Falcon** to analyze the execution flow. The malicious macro had downloaded a script that executed PowerShell commands.

Phase 3: Credential Access (T1003.001 – LSASS Memory Dumping)

Using **EDR logs**, the team found that Mimikatz was executed, attempting to extract login credentials. The attacker aimed to escalate privileges.

Phase 4: Lateral Movement (T1021.002 – SMB Admin Shares)

The attacker then attempted to move across the network using stolen credentials. The SOC team, monitoring network logs via **Zeek**, identified unusual SMB traffic between multiple workstations.

Phase 5: Containment and Eradication

- **Isolated the infected machine** to prevent further movement.
- **Reset compromised credentials** and forced multi-factor authentication.
- **Used Palo Alto firewalls** to block the attacker's command-and-control IP.
- **Performed forensic analysis** using Volatility to confirm the attacker's tactics.

Phase 6: Mitigation and Lessons Learned

- **Enhanced email filtering** to detect phishing emails.
- **Implemented stricter PowerShell execution policies** to prevent script-based attacks.
- **Conducted cybersecurity training** for employees on recognizing phishing attempts.

6. Conclusion

The **MITRE ATT&CK framework** is essential for understanding attacker behavior, improving security defenses, and fine-tuning **SIEM alerts** for real-time detection. By leveraging ATT&CK, organizations can **detect, investigate, and respond** to threats more effectively, reducing the risk of cyber incidents.