

Mitre attack framework

Reported By Cyber Assassins

**Team member names**

October 8, 2025

Syed Danyal Raza

Abeeha Israr

Basim Nawaz

Fasieha

Muhammad Sameed Asif



**Introduction to MITRE ATT&CK:**

In this fast-growing world where access to the internet is available to everyone, the chances of cyber-attacks have increased. Threat actors are using advanced techniques called **Advanced Persistent Threats** (APTs). Obviously old techniques are not enough because threat actors use different techniques each time for different companies.

Now MITRE, which is an open-source organization, is coming into the game. In 2013, they introduced a framework which is called **MITRE FRAMEWORK** which keeps track of every group of threat actors. This framework consists of **TTPs** (tactics, techniques and procedures).

**Advantages of MITRE ATT&CK Framework:**

There are other frameworks too, but why do we prefer MITRE in special is because of these reasons:

* It helps security professionals in threat detection, incident response & vulnerability management.
* It is open source and additionally uses public domain so that everyone can use it and check and strengthen their security measures and controls.
* It consists of 14 tactics and many techniques so every real-world cyber-attack can be covered in these.
* It offers different matrices for different operating systems (OS) such as Linux, windows etc.

**Case Studies: Applying the MITRE ATT&CK Framework:**

1. **Case-1: Individual Level**

* **Targeted individual type:**

Threat actor targets an individual who is working at a prestigious bank and holds a senior position.

* **Potential gains from attack:**

Threat actors want to gain access to sensitive personally identifiable information (SPII) to gain financial benefits.

* **Scenario:**

That targeted person receives an email from a similar name to the company has. A person holds a senior position and has SPII data in his system. He carefully goes through the email, looks at the domain attached, and other relevant things and mistakes it for an official email from the head office. He clicks the link that asks for some fishy thing kind of verification stuff and boom, as soon as that link opens in the browser, a cyber-attack occurs. The installation of malware starts, and software used to steal information starts its processing.

A threat actor becomes successful in his mission, and he now has all the SPII. He can use this SPII to gain:

* Financial benefits
* Blackmail the people
* Sell that data
* **TTPs of MITRE ATT&CK Framework:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tactics** | **Techniques used** | **MITRE ATT&CK ID** | **Procedure** |
| Reconnaissance | Social engineering | T1566.001 | Threat actor will gather information about that individual from his social media and other platforms |
| Initial access | Phishing  Spear-phishing Link | T1566.002 | They will share some infected email or link having malware |
| Execution | User Execution | T1204 | Trick users in such a way that they are forced to open infected link |
| Persistence | Account  Manipulation | T1098 | Threat actor will try to change passwords of system so that user can’t access it |
| Defense evasion | Indicator Removal on Host | T1070 | Disable security tools  Delete security logs & other details |
| Credential access | Two-Factor Authentication Intercepting | T1111 | Capture or bypass system’s passwords using 2FA codes |
| Discovery | Account Discovery | T1087 | They go through the data and see which user account still exists |
| Collection | Keylogging | T1056.001 | They are recording and looking at what victim is doing/typing after system is compromised |
| Command & control | Encrypted Channel | T1573 | They communicate with encryption so that security tools can’t read |
| Exfiltration | Automated Exfiltration | T1020 | They use scripts or tools to automatically transfer data |
| Impact | Data Destruction | T1485 | Use tools to delete files permanently so that user can’t recover |

* **How to prevent such attacks using MITRE ATT&CK Framework:**
* Regularly check the event viewer of your system. Keep an eye on security logs and check what activity is going on
* Use security tools like SIEM to detect the activity and logs
* Check the user accounts and local groups created on your system using command prompt.
* Always secure your user account with passwords

1. **Case-2: Medium-sized organization**

* **Targeted organization type:**

A medium-sized software development company that provides cloud-based project management tools to its clients.

* **Potential gains from attack:**

The threat actor aims to deploy ransomware across the company’s file servers and endpoints to:

* Disrupt business operations.
* Demand a ransom payment in cryptocurrency.
* Potentially exfiltrate sensitive client data to sell on the dark web if ransom isn’t paid.
* **Scenario:**

The attackers perform reconnaissance on the company’s public-facing infrastructure and discover that the company has a self-hosted VPN portal for remote employees. The VPN software version is outdated and vulnerable to a known remote code execution (RCE) flaw.

The attacker exploits this VPN vulnerability to gain a foothold inside the company network. Once inside, they escalate privileges using stolen admin credentials found in unsecured configuration files. With administrative access, the attacker moves laterally through the network, encrypts file servers, and exfiltrates client data before encryption begins.

A ransom note is left on all affected machines, demanding payment to restore access.

* **TTPs of MITRE ATT&CK Framework:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tactics** | **Techniques** | **MITRE ATT&CK ID** | **Procedure** |
| Initial Access | Exploit Public-Facing Application | T1190 | Attackers exploit an unpatched VPN vulnerability to gain initial foothold. |
| Execution | Command and Scripting Interpreter (PowerShell) | T1059.001 | Uses PowerShell scripts to deploy ransomware payloads. |
| Privilege Escalation | Exploitation for Privilege Escalation | T1068 | Leverages local privilege escalate vulnerability to gain admin rights. |
| Credential Access | Unsecured Credentials | T1552 | Reads plaintext admin credentials stored in configuration files. |
| Lateral Movement | Remote Services (SMB/WinRM) | T1021 | Uses stolen credentials to move across servers and endpoints. |
| Collection | Archive Collected Data | T1560 | Compresses sensitive client data before exfiltration. |
| Exfiltration | Exfiltration Over Web Services | T1567 | Transfers stolen data to cloud storage controlled by attacker. |
| Impact | Data Encrypted for Impact | T1486 | Encrypts company file servers and endpoints, halting operations. |

* **How to prevent such attacks using MITRE ATT&CK Framework:**
* Keep all public-facing applications (VPN, web apps) up to date with the latest security patches.
* Perform regular scans on external-facing systems to detect and remediate exploitable flaws.
* Remove unnecessary admin privileges and store credentials securely using password vaults.
* Enforce MFA for VPN and remote services to reduce credential-based compromise risk.
* Separate critical servers from employee endpoints to slow lateral movement.
* Deploy SIEM/EDR solutions to detect unusual PowerShell execution, large outbound data transfers, and multiple failed login attempts.
* Have a ransomware-specific response plan to isolate infected machines and restore backups quickly.

1. **Case-3: Large Enterprise**

* **Targeted organization type:**

A large multinational corporation with a dedicated finance department responsible for handling high-value transactions and vendor payments.

* **Potential gains from attack:**

The threat actor aims to initiate a fraudulent wire transfer to an account under their control, leading to:

* Significant financial loss for the organization.
* Disruption of business operations.
* Potential reputational damage if fraud becomes public.
* **Scenario:**

The attacker conducts reconnaissance to identify high-ranking executives, such as the CEO or CFO, and employees within the finance department. They then craft highly convincing phishing emails or spoofed messages impersonating the executive, instructing the finance team to urgently process a wire transfer to a specified account.

Believing the request to be legitimate, and under pressure from the perceived authority of the sender, finance staff proceed with the transfer without secondary verification.

By the time the real executive becomes aware and questions the transaction, the funds have already been transferred to an attacker-controlled account.

This attack commonly leverages:

* Social Engineering to manipulate employees’ trust.
* Business Email Compromise (BEC) to send convincing fraudulent requests.
* Compromised Credentials to access legitimate email accounts and communication threads.
* **TTPs of MITRE ATT&CK Framework:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tactics** | **Techniques** | **MITRE ATT&CK ID** | **Procedure** |
| Initial access | Phishing | T1566 | Using spear-phishing emails to steal credentials or deliver malware to compromise accounts. |
| Valid Accounts | T1586 | Gaining unauthorized access to legitimate email accounts through credential theft or phishing. |
| Execution | Spear-phishing via Service | T1566.002 | Sending targeted phishing emails using legitimate business communication platforms to deceive recipients. |
| Persistence | Account Hijacking | T1098 | Maintaining access to compromised email accounts to continue fraudulent activities. |
| Defense Evasion | Email Address Spoofing | T1609 | Creating email addresses that closely mimic legitimate executives’ addresses to evade detection. |
| Impersonation | T1656 | Impersonating high-level executives or trusted vendors to manipulate recipients into unauthorized actions. |
| Collection | Email Collection | T1114 | Accessing email communications to gather intelligence and further impersonate targets. |

* **How to prevent such attacks using MITRE ATT&CK Framework:**
* Deploy advanced email security solutions with anti-phishing capabilities to detect and block spear-phishing emails.
* Enforce multi-factor authentication (MFA) for all email accounts, especially for executives and finance personnel, to prevent unauthorized use of valid accounts.
* Implement email gateway protections to identify and filter spoofed emails.
* Enable security information and event management (SIEM) tools to correlate suspicious email activities and generate timely alerts.
* Regularly audit and review access permissions, especially for email accounts with financial approval authority.

**Conclusion:**

These three scenarios demonstrate that while the scale and complexity of cyber-attacks vary depending on the size and nature of the target, the **MITRE ATT&CK framework** provides a consistent method to map, analyze, and mitigate adversary behavior.

* **For individuals** (Case 1), the main risks stem from **social engineering and malware delivery**, emphasizing the need for strong phishing awareness and endpoint protection.
* **For medium-sized organizations** (Case 2), vulnerabilities in **public-facing applications** present high-risk entry points, making patch management and access control essential.
* **For large enterprises** (Case 3), **BEC and impersonation attacks** exploit human trust within critical departments, highlighting the importance of multi-factor authentication, strict transaction verification processes, and advanced email security.

Ultimately, regardless of the target’s size, a layered security approach combining technical defenses, user awareness, incident response readiness, and continuous monitoring is critical. The MITRE ATT&CK framework not only helps in post-incident analysis but also guides proactive defense strategies to reduce the likelihood and impact of future attacks.