**Understanding Mitre Att&ck**

Mitre Att&ck is a non-profit knowledge base funded by the US federal government. Att&ck here stands for Adversarial Tactics, Techniques, and Common Knowledge. It works with the private industry and the US government. This has a mission of solving problems for a safer world by bringing communities together to develop more effective cybersecurity. It is an accessible knowledge base of different ways and methods which are based on real-life situations. This is used worldwide. They have done tons of work in various fields like counterterrorism, bank fraud, cybersecurity, etc. MITRE is familiar with maintaining the common vulnerabilities and exposures (CVE) list super valuable input for vulnerability management technology around the world.

Mitre Att&ck consists of three matrices, Pre-Att&ck, Att&ck, and Mobile. They together comprise an end-to-end attack chain that is filled with all kinds of successful techniques that adversaries use to breach organizations and tamper with confidential data. While the concept of the attack chain is not new, the visibility into the confirmed techniques provides information to blue teams that previously was only reserved for elite incident responders or otherwise classified information.

**How does it start?**

It starts with initial reconnaissance and scouting out the delivery mechanism, whether it be phishing or malware with Pre-Att&ck, and once the adversary has internal access to the network, certainly that privilege escalation, lateral movement, data exfiltration, and ending with command and control.

**The Contextual Term Meaning of Att&ck**

**1)Tactics**

This points to the objective of the attackers. What the attacker is trying to get, whether it is the data access, control mechanism, or maintaining persistence. When an attacker is trying to attack an organization, they must use different tactics to get success in their attack.

**2)Techniques**

After ‘what’ comes the ‘How’. This term mainly describes how the attackers are executing their tactics. Attackers have various techniques to fulfill their tactics. These techniques are divided into subdivisions. To cite an example, the concept of phishing can be taken. Although the tactics or the reason for the attack is generally to get access to confidential data, the phishing technique is subdivided roughly into three parts.

**3)Procedures**

This mainly describes the applications of techniques and sub-techniques. It can also point to the viruses or malware that the attacker might have used.

**Who can use this?**

Since this is a cost-free tool, various organizations of varied sizes use this tool efficiently. Both private and public sector organizations use this tool. The users also belong to different categories like cyber security management teams, red teams, blue teams, security defenders, teams looking forward to building applications and providing services, etc. The reason this is valuable to blue teams is that this can be mapped against current detection and data collection in the environment.

A lot of teams are taking a step further by emulating for example Advanced Persistent Threats (APT) and seeing a true risk of these techniques in their internal environment.

**Why is this useful?**

1) The thing to consider is that this is focused on protecting the internal network for compromise. If something has to be monitored, for example, infrastructure as a service or web applications, the techniques to be used should be prioritized to match the frequent attacks on the organization.

2)It is not just a list of techniques. Instead of thinking that the attacker only needs to be right once to successfully get in and breach a company, it can be flipped in its head by the attacker only needing to slip up or detected once for the blue teams to figure out and remove it.

3)It is shedding a lot of light on confirmed attacks and breaching.

**References**

1)<https://attack.mitre.org/>

2)<https://www.rapid7.com/fundamentals/mitre-attack/>

3)<https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html>

4)<https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful>

5)<https://www.f5.com/labs/articles/education/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why>

6)<https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/>

7)<https://www.vmware.com/topics/glossary/content/mitre-attack.html>