CASE STUDY

INTRODUCTION -

The knowledge base and all the pertinent methodologies in the MITRE ATT&CK are based on real-world observations, and it is accessible from anywhere in the world. The creation of various sophisticated threat models in both the public and private sectors is also supported by the ATT&CK knowledge base. Additionally, the cybersecurity community uses them.

The creation of the ATT&CK has allowed for its application in various real-time settings to solve issues. As a result, the communities may work together to create security frameworks and policies that are more effective. The ATT&CK is open-source and available to developers without payment for resource updates. The technical goal of what the attackers are attempting to accomplish is frequently referred to as the tactics. Examples include obtaining credentials, keeping up persistence, or exercising command and control. To successfully carry out an attack, the attackers frequently employed several strategies.

ROLE OF ATT&CK IN THE ORGANIZATION -

The blue team utilizes the same ATT&CK to attempt and defend the systems and counter the attack plans of the red team, while the red team uses it to construct a plan utilizing various approaches to test the attack's efficiency. The top-level category in the MITRE is referred to as "techniques," and the MITRE ATT&CK is a repository of knowledge about the nefarious tactics employed by advanced persistent threat groups (APT) at various phases of real-time cyber attacks.

Cyberthreat Intelligence Enrichment: This would be beneficial to improve knowledge about specific dangers and threat actors. To determine whether they need to strengthen the protection mechanisms against particular APTs, the defenders can read the scenario and analyze it using ATT&CK (advanced persistent threats).

Red teaming: This serves as a vehicle to illustrate the consequences of a breach. The red team can use ATT&CK to develop specific plans for organizing and planning successful operations.

These are some of the ways that organizations use MITRE ATT&CK.

The security teams in the organization are examining the MITRE ATT&CK and creating methods of detection and preventative control for the enterprise matrix due to the present effects of the previous attack.

Some of the techniques onboarded in the organization are -

INITIAL ACCESS -

Several alternative strategies are utilized to get access to the network during the initial access. These include techniques like exploiting web server vulnerabilities and targeted spear phishing. Further access would be made possible by this network action, including the use of legitimate accounts and the creation of external remote services.

EXECUTION -

Techniques that have controlled code running on a system make up the execution phase. This could be a distant or local system within the company. These are frequently combined with other malicious activities to give more access to the network. This might be accomplished in a number of ways, like by utilizing a remote access tool to execute a PowerShell script that locates distant computers.

PERSISTENCE -

In the persistence phase, specific methods are used to maintain access to the systems. Even if the machine is restarted or the user credentials change, this would still be eligible, even though some disruptions would prevent connection to the network. The phase uses methods like action and access. They might keep control of the computers by making certain code modifications, such as hijacking legal code or adding startup code.

PRIVILEGE ESCALATION -

The privilege escalation step involves using certain methods to obtain higher-level access to the network or its systems. This would make it easier to examine a network with limited access. Certain permissions that accomplish their goals would be necessary for this. One of the main strategies is to exploit system flaws, incorrect setups, and specific vulnerabilities.

- SYSTEM/root level
- local administrator
- user account with admin-like access

These techniques often overlap with persistence techniques.

DEFENSE EVASION -

Several methods are employed in the defense evasion phase to prevent detection across all compromised systems. Deleting the security software is one of the defense evasion strategies. Through this procedure, the security software may occasionally be disabled. This would also address the consequences of malware authors abusing trusted processes to conceal and disguise it.

PRIORITIES ON ON-BOARDING THE FRAMEWORK -

The framework has been onboarded into the organization. Looking for the effectiveness of the working application, the system is often onboarded step by step, with certain implementations at every step. To utilize ATT&CK, the red team develops certain strategies to link together to test the defenses of their targets. The blue team needs to understand certain tactics used by the red team in order to counter their strategies and provide effective solutions. With consideration of different levels of implementation, each framework is onboarded at a specific time to effectively increase the success rate of security standards in organizations.

INITIAL ACCESS -

Several methods are employed in the defense evasion phase to prevent detection across all compromised systems. Deleting the security software is one of the defense evasion strategies. Through this procedure, the security software may occasionally be disabled. This would also address the consequences of malware authors abusing trusted processes to conceal and disguise it. Examples - T1189 Drive-by Compromise.

EXECUTION -

All of the various execution methods make use of specific commands to run scripts, binaries, and other programs. Different ways to interact with the systems are provided by these interfaces and languages, and specific functionality are accessible on various platforms. The majority of these systems include built-in command-line interfaces that are accessible across various Linux and macOS distributions.

Examples - T1059,T1059 - Command and Scripting Interpreter. T1001- Powershell.

PERSISTENCE -

The persistence phase's methods can be used to alter accounts in order to continue having access to victim systems. An activity that can jeopardize an account, such as changing the credentials, is called account manipulation. These acts may also cause activity to be directed away from the rules of current security. This further results in credentials being compromised and password bypassing.

Examples - T1098 - account manipulation.

PRIVILEGE ESCALATION -

Mechanisms created to manage specific rights in order to obtain particular high-level permissions make up the phase of privilege escalation. The majority of systems have specific authorization mechanisms in place to safeguard user rights and restrict their use. The idea of giving individual users permission to carry out designated duties is thought to pose a higher risk. To increase a user's privileges on a system, built-in commands that come with specific mechanisms are utilized.

Examples - T1548, - Abuse Elevation Control Mechanism."

DEFENSE EVASION -

The phase includes specific controls for the enhanced privileges that are achieved in order to obtain higher level permissions. The majority of contemporary systems have some features that use native elevation control techniques to restrict the rights that a particular user may exercise on the system. The ability to carry out particular tasks on systems that pose a higher risk must be allowed to a small group of users.

Examples - T1548, - Abuse Elevation Control Mechanism."

These steps are implemented in a sequential manner, to provide the organization with effective results and further study the implementation and strategic results.

Business value provided by the organization :

The ATT&CK structure was implemented in the organization's current repository for a number of reasons, one of which is that it gives the red team useful group listings for organizing and using the most recent tools and strategies to infiltrate the organization's targets.

Considering a few instances of the entries for various groups, the attack methods include scheduled tasks, remote file copy, and command-line interfaces. Even though

One of the approaches is on the short side, but it would still be used in the technique description and may be used in many examples.

- This uses real-world software and scenarios that are obtained from the group lists.
- These help socialize and share the ATT&CK techniques in the same language as the security systems.
- These help with identifying the gaps that are helped by defenses in the system with the ATT&CK matrices and implementing the solutions for those gaps.
- Although one can defend against an attack, this doesn't always mean that they can defend against different attacks in the same systematic scenario.

REFERENCES -

MITRE ATT&CK -

https://attack.mitre.org/