Write-up: "ATT&CK" Challenge – Blue Team Labs Online

The "ATT&CK" challenge from Blue Team Labs Online (BTLO) is designed to develop threat intelligence and blue team analysis skills through the practical use of the MITRE ATT&CK framework. Participants are required to answer a series of questions based on real-world scenarios by exploring the ATT&CK knowledge base to identify adversary behaviors, techniques, and procedures.

Scenario

You are hired as a Blue Team member for a company. You are assigned to perform threat intelligence for the company. See how you can operationalize the MITRE ATT&CK framework to solve these scenario-based problems.

Questions:

Your company heavily relies on cloud services like Azure AD, and Office 365 publicly. What technique should you focus on mitigating, to prevent an attacker performing Discovery activities if they have obtained valid credentials? (Hint: Not using an API to interact with the cloud environment!)

Answer: T1538 – Cloud Service Dashboard

Explanation:
Using the Enterprise ATT&CK matrix, under the "Reconnaissance" tactic, you can locate technique T1538, which describes adversaries accessing web-based cloud dashboards to gather information about services and configurations. This technique refers to the use of cloud service graphical user interfaces (GUIs) to obtain information about the operating environment, without the need for APIs.

You were analyzing a log and found uncommon data flow on port 4050. What APT group might this be?

Answer: G0099

Using the ATT&CK *Groups* section, in the group profile, it is documented that APT-C-36 (G0099, a South American threat actor) has used port 4050 for command and control (C2) communications.

The framework has a list of 9 techniques that falls under the tactic to try to get into your network. What is the tactic ID?

Answer: TA0001 – Initial Access

Explanation: This tactic encompasses methods adversaries use to gain initial access to a network, such as phishing, vulnerability exploitation, and others.

A software prohibits users from accessing their account by deleting, locking the user account, changing password etc. What such software has been documented by the framework?

Answer: S0372 – LockerGoga

Explanation:

In the Software section, the description of LockerGoga states that it is a ransomware variant, known for modifying account credentials or disabling access as part of its destructive behavior.

Using 'Pass the Hash' technique to enter and control remote systems on a network is common. How would you detect it in your company?

Answer: Monitor newly created logons and credentials used in events and review for discrepancies.

Navigating to subtechnique T1550.002 – Pass the Hash in the ATT&CK matrix, under "Detection", it recommends monitor newly created logons and credentials used in events and review for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity.