ATT&CK-Blueteam lab

Scenario

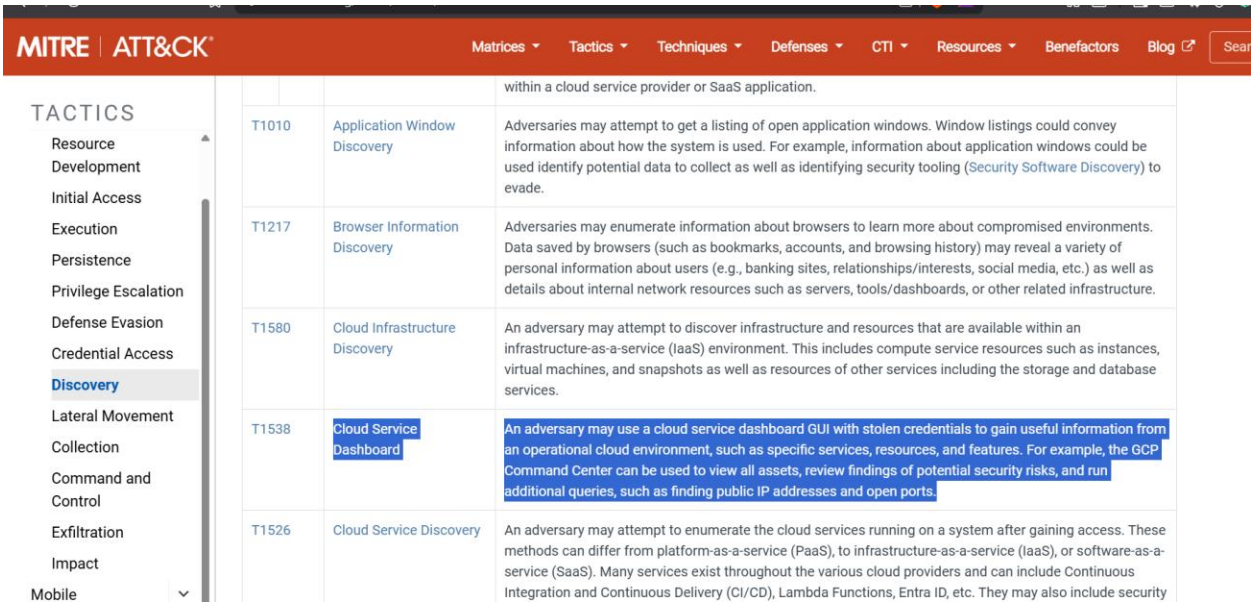
You are hired as a Blue Team member for a company. You are assigned to perform threat intelligence for the company. See how you can operationalize the MITRE ATT&CK framework to solve these scenario-based problems.

Q1. 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

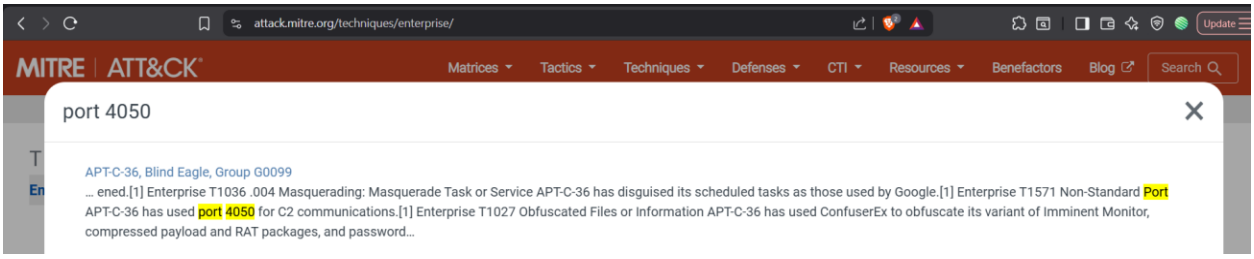
Description

The adversary attempts to gain an initial foothold within the target environment



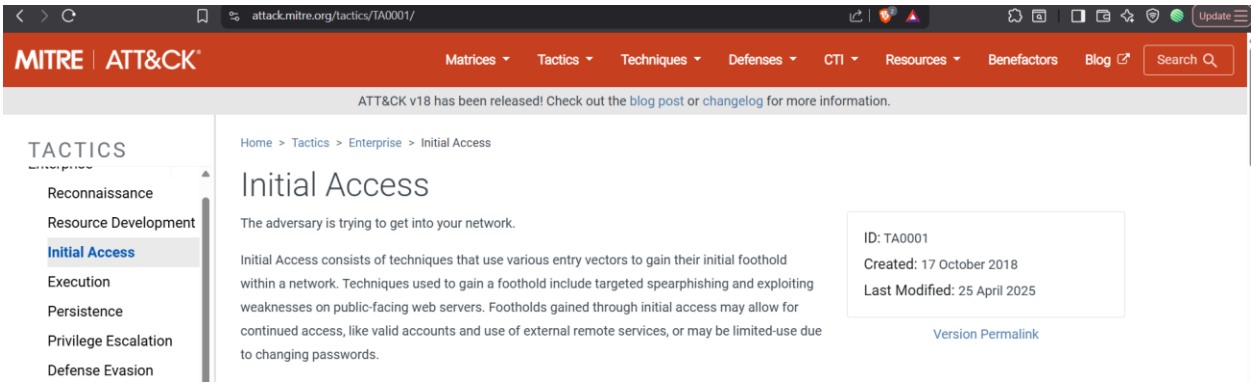
Q2-You were analyzing a log and found uncommon data flow on port 4050. What APT group might this be? Answer/G0099

Port **4050** is a non-standard network port commonly abused by attackers for **Command and Control (C2) communication**. It has been observed in APT activity to maintain remote access, evade detection, and exchange malicious commands between compromised systems and attacker servers.



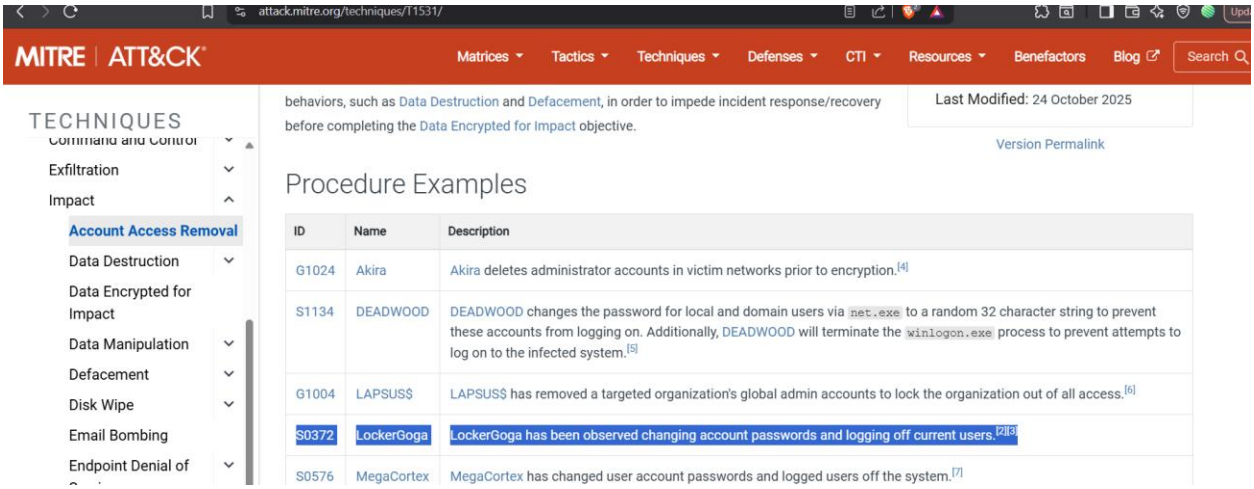
Q3-The framework has a list of 9 techniques that falls under the tactic to try to get into your network. What is the tactic ID? answer/TA001

Initial Access (TA0001) refers to the techniques attackers use to gain their first entry into a target environment. This includes methods such as phishing, exploiting public-facing applications, brute-force attacks, or using stolen credentials to establish an initial foothold in the network.



Q4-A software prohibits users from accessing their account by deleting, locking the user account, changing password etc. What such software has been dcumented by the framework? Answer/S0372

Account Access Removal (T1531) is an impact technique where attackers delete user accounts or change account passwords to block legitimate users from accessing their systems. This is commonly used to disrupt operations, delay incident response, and maintain attacker control over the environment.



Q5-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