

## ATT&CK

**Platform:** blueteamlabs.online

**From:** Asem Reda

**Diploma:** Cybersecurity 87

**Challenge link:** <https://blueteamlabs.online/home/challenge/attck-0e4914db5d>

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.

### Challenge Submission

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!) (2 points)

Solved!

You were analyzing a log and found uncommon data flow on port 4050. What APT group might this be? (2 points)

Solved!

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? (2 points)

Solved!

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? (2 points)

Solved!

Using 'Pass the Hash' technique to enter and control remote systems on a network is common. How would you detect it in your company? (2 points)

Solved!

## Task1:

Solution steps:

Open MITRE ATT&CK

Select Techniques → Enterprise → Cloud

Under Discovery, search for each technology individually

The only one that mentions: **“without making API requests”**

She:

T1538 – Cloud Service Dashboard

The screenshot shows the MITRE ATT&CK Cloud Service Dashboard. The left sidebar lists various techniques under the 'Discovery' category, with 'Cloud Service Dashboard' selected. The main content area displays the title 'Cloud Service Dashboard' and a description: 'An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, review findings of potential security risks, and run additional queries, such as finding public IP addresses and open ports.[1]'. Below this, it states: 'Depending on the configuration of the environment, an adversary may be able to enumerate more information via the graphical dashboard than an API. **This also allows the adversary to gain information without manually making any API requests.**'. A right-hand panel provides metadata: ID: T1538, Sub-techniques: No sub-techniques, Tactic: Discovery, Platforms: IaaS, Identity Provider, Office Suite, SaaS, Contributors: Obsidian Security, Praetorian, Version: 1.5, Created: 30 August 2019, Last Modified: 24 October 2025. A 'Version Permalink' link is also present. At the bottom, there is a 'Procedure Examples' section with a table.

ID	Name	Description
T1538	Cloud Service Dashboard	Cloud Service Dashboard: An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, review findings of potential security risks, and run additional queries, such as finding public IP addresses and open ports.[1]

## Task 2:

Solution steps:

Go to CTI, then select Groups, then type port 4050 in the search bar. You will find the group name G0099 — APT-C-36

The screenshot shows the MITRE ATT&CK CTI Groups page. A search bar at the top contains the text 'port 4050'. Below the search bar, a list of groups is displayed, with 'G0099' (APT-C-36) highlighted. The description for G0099 is: 'APT-C-36, Blind Eagle, Group G0099 ... ened.[1] Enterprise T1036\_004 Masquerading: Masquerade Task or Service APT-C-36 has disguised its scheduled tasks as those used by Google.[1] Enterprise T1571 Non-Standard Port APT-C-36 has used port 4050 for C2 communications.[1] Enterprise T1027 Obfuscated Files or Information APT-C-36 has used ConfuserEx to obfuscate its variant of Imminent Monitor, compressed payload and RAT packages, and password...'. Below the search results, there is a section titled 'Associated Group Descriptions' with a table.

Name	Description
Blind Eagle	[1]

At the bottom, there is a section titled 'Techniques Used' with a button labeled 'ATT&CK® Navigator Layers'.

### Task 3:

Solution steps:

The question states:

"The framework has a list of techniques that fall under the tactic where the adversary is trying to get into your network"

Focusing on the phrase:

"trying to get into your network"

This means: The attacker is still outside the network... and still trying to get in

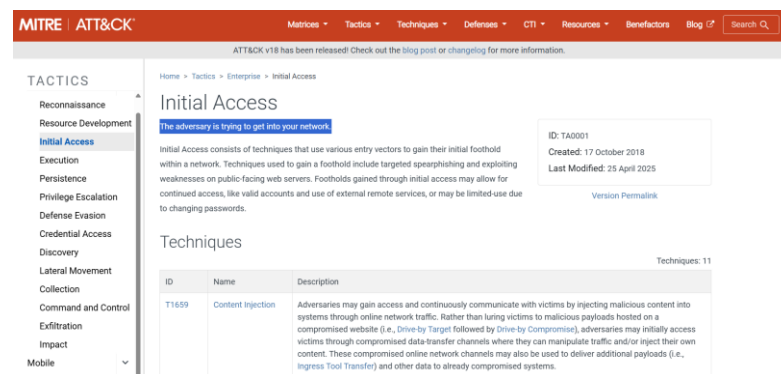
This stage is **Initial Access** because its goal is to attempt to gain access to the network

The text within MITRE confirms this

If you open the MITRE website to Initial Access, you will find the following

"The adversary is trying to get into your network"

This is the same sentence as the question



### Task4:

Solution steps:

First, we must identify the technique that describes this behavior, and then we can see which program uses this technique.

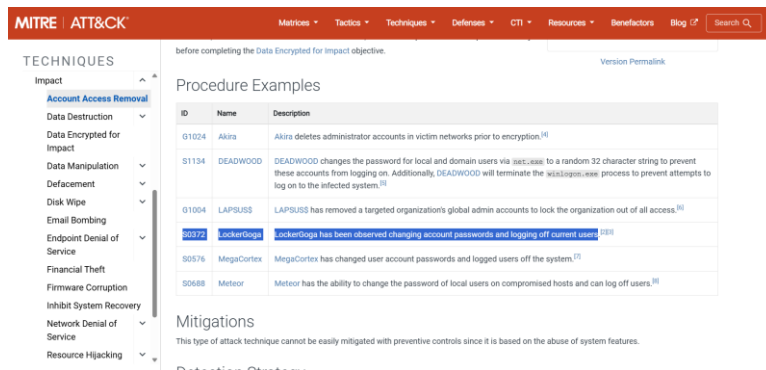
Next, go to the Techniques menu and select Enterprise.

In the search bar, enter keywords like "deleted" and "locked," similar to those mentioned in the question.

Select T1531 because its description matches the question.

Then, scroll down to the Procedure Examples section and you'll find that **"S0372**

**LockerGoga has been observed changing account passwords and logging off current users"**



## Task 5:

First, type "Pass the Hash" in the search bar, then select "Detection Strategy for T1550.002 - Pass the Hash (Windows), Detection Strategy DET0409." Next, scroll down to "Analytics Windows AN1144" and read the text. You will find that the answer is **"Monitor newly created logons and credentials used in events and review for discrepancies"**

## Summary of the pass the hash page:

It tells you to:

1. Monitor for unusual NTLM logins
2. Monitor for new Logon sessions
3. Monitor if the user is logging into an unusual machine
4. Interrelate all of this information
5. Use Windows + Sysmon events for detection

