MITRE ATT&CK Framework – Threat Intelligence Report

BlueTeamLabs Challenge

Student Name: Romaissaa Moftah

Course: Cybersecurity / Blue Team / Threat Intelligence

Instructor: Eng. Taha Abouelhgag

1. Executive Summary

This report documents the operational use of the MITRE ATT&CK Framework to perform threat intelligence analysis for a cloud-reliant organization. The investigation focuses on mapping real-world security scenarios to ATT&CK tactics, techniques, and adversary groups. By correlating suspicious behaviors, ports, malware, and credential abuse techniques, this analysis demonstrates how defenders can proactively detect, classify, and mitigate threats across enterprise and cloud environments.

2. Case Overview

The organization heavily relies on cloud services such as Azure Active Directory and Office 365. As a Blue Team analyst, the primary objective is to identify potential adversary techniques, determine threat actor associations, and recommend effective detection and mitigation strategies. The scenarios provided simulate common attacker behaviors such as credential abuse, command and control communication, account disruption, and lateral movement.

3. Tools and Methodology

The following tools and resources were used during the investigation:

- MITRE ATT&CK Framework (https://attack.mitre.org/)

- Google Hacking for open-source threat intelligence (OSINT)

- Threat intelligence references and adversary group documentation

- Log analysis concepts and credential monitoring techniques

The methodology involved mapping each scenario to the appropriate MITRE ATT&CK tactic and technique, identifying known threat actor associations, and recommending detection and mitigation strategies aligned with industry best practices.

4. Step-by-Step Analysis

4.1 Cloud Discovery Using Stolen Credentials

Scenario:

The company relies on Azure AD and Office 365 publicly. An attacker has obtained valid credentials and attempts to perform discovery without using an API.

Analysis:

The attacker is likely using the cloud service graphical user interface (GUI), such as the Azure Portal or Office 365 Admin Center, to enumerate users, roles, and configuration settings.

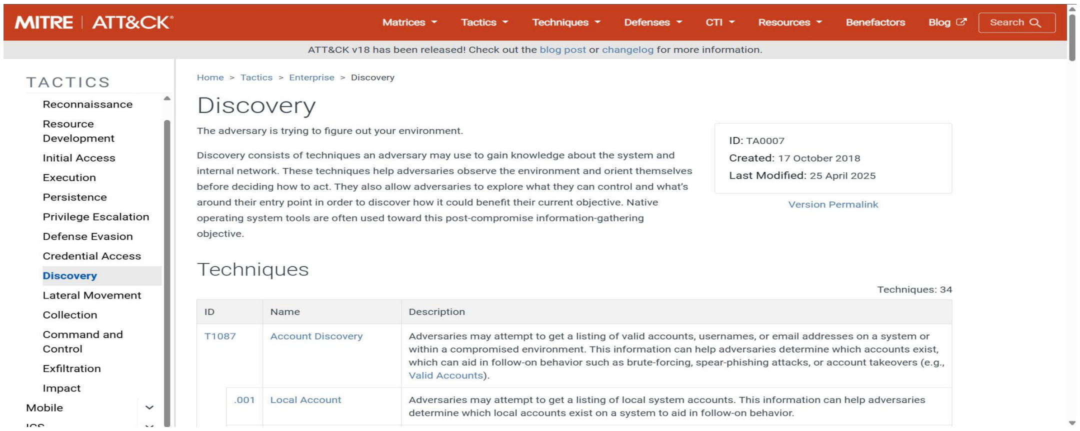
MITRE Mapping:

Technique ID: T1538

Tactic: Discovery

Explanation:

This technique focuses on adversaries leveraging cloud service management interfaces to gather information about the environment using stolen credentials, rather than interacting directly through APIs. The attacker may enumerate accounts, permissions, and resources to identify high-value targets.



ATT&CK v18 has been released! Check out the blog post or changelog for more information.

Discovery

The adversary is trying to figure out your environment.

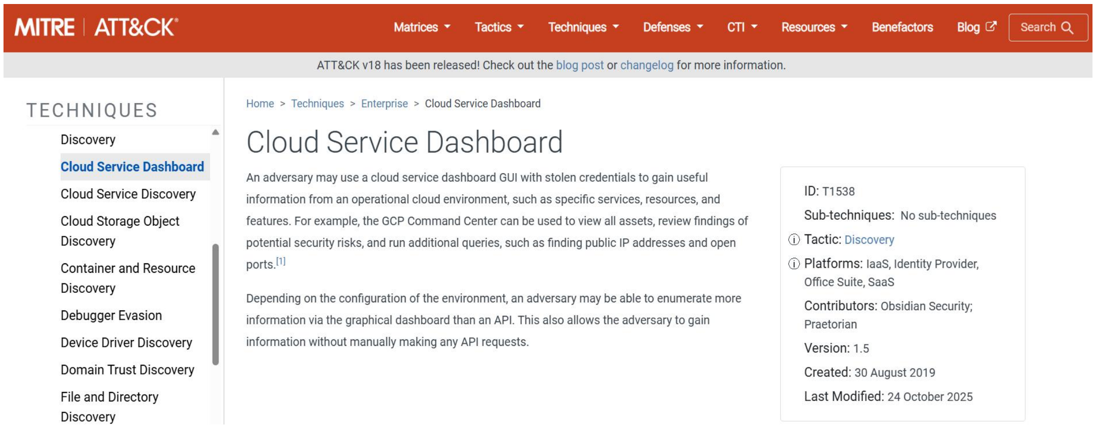
Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

ID: TA0007
Created: 17 October 2018
Last Modified: 25 April 2025

Techniques

Techniques: 34

ID	Name	Description
T1087	Account Discovery	Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., Valid Accounts).
.001	Local Account	Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.



ATT&CK v18 has been released! Check out the blog post or changelog for more information.

Home > Techniques > Enterprise > 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]

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.

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

4.2 Uncommon Network Traffic on Port 4050

Scenario:

Log analysis reveals suspicious outbound traffic on port 4050.

Analysis:

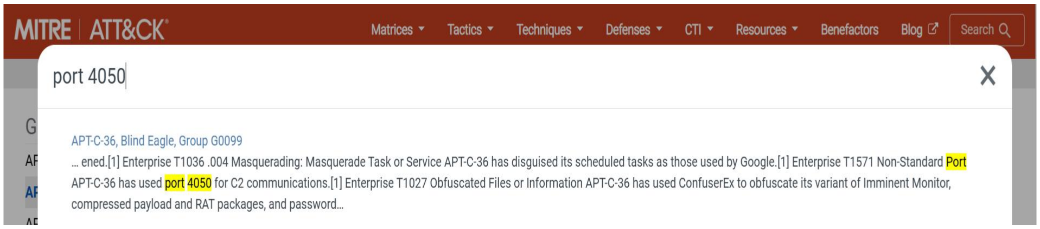
Threat intelligence research indicates that this port has been used by specific advanced persistent threat (APT) groups for command and control (C2) communications.

MITRE Mapping:

APT Group: G0099 (APT-C-36)

Explanation:

APT-C-36 has been documented using port 4050 as part of its command and control infrastructure. The presence of traffic on this port suggests potential compromise and active remote communication with an adversary-controlled server.



port 4050

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…

4.3 Identifying the Initial Access Tactic

Scenario:

The framework lists techniques focused on gaining entry into the network.

Analysis:

This set of techniques falls under the Initial Access tactic, which describes how attackers attempt to breach an organization’s defenses and gain a foothold within the environment.

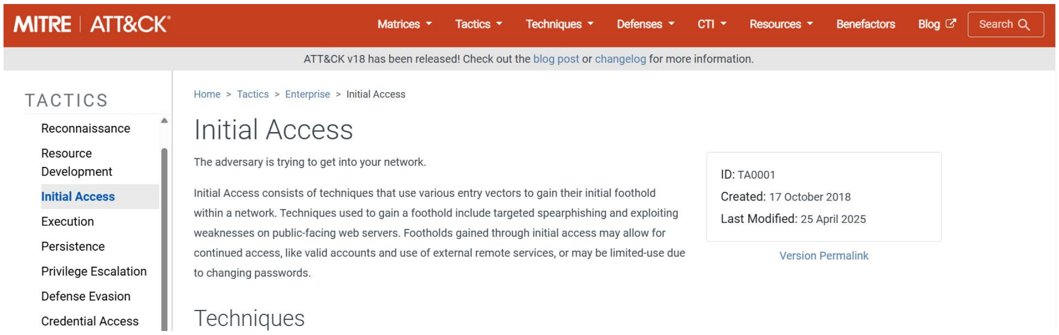
MITRE Mapping:

Tactic ID: TA001

Tactic Name: Initial Access

Explanation:

This tactic includes methods such as phishing, exploiting public-facing applications, and using valid accounts to gain entry into the network.



ATT&CK v18 has been released! Check out the blog post or changelog for more information.

Home > Tactics > Enterprise > Initial Access

Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

ID: TA0001
Created: 17 October 2018
Last Modified: 25 April 2025

Version Permalink

Techniques

4.4 Account Locking and Disruption Malware

Scenario:

A software application deletes user accounts, locks access, and changes passwords to deny legitimate user access.

Analysis:

This behavior aligns with destructive ransomware and locker-style malware designed to disrupt operations and deny access to systems.

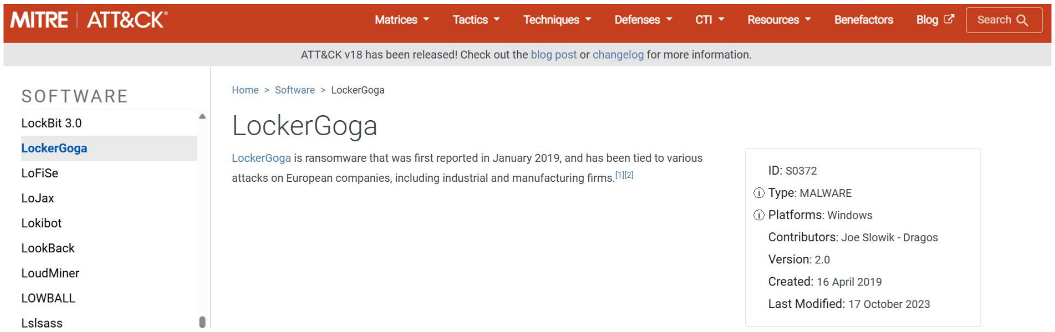
MITRE Mapping:

Software ID: S0372

Malware Name: LockerGoga

Explanation:

LockerGoga is known for locking user accounts and disrupting authentication mechanisms, often used in ransomware campaigns to halt business operations and pressure organizations into paying ransoms.

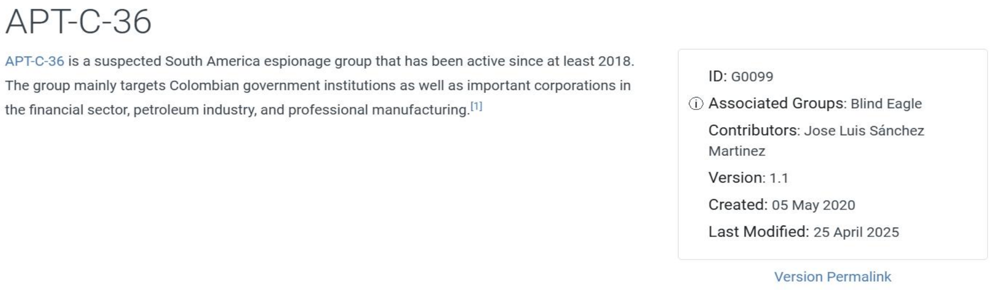


ATT&CK v18 has been released! Check out the blog post or changelog for more information.

LockerGoga

LockerGoga is ransomware that was first reported in January 2019, and has been tied to various attacks on European companies, including industrial and manufacturing firms.[1][2]

ID: S0372
ⓘ Type: MALWARE
ⓘ Platforms: Windows
Contributors: Joe Slowik - Dragos
Version: 2.0
Created: 16 April 2019
Last Modified: 17 October 2023



APT-C-36

APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.[1]

ID: G0099
ⓘ Associated Groups: Blind Eagle
Contributors: Jose Luis Sánchez Martinez
Version: 1.1
Created: 05 May 2020
Last Modified: 25 April 2025

4.5 Detection of Pass-the-Hash Attacks

Scenario:

An attacker uses the Pass-the-Hash technique to remotely access and control systems within the network.

Analysis:

This technique allows attackers to authenticate using stolen password hashes without knowing the actual plaintext password.

Detection Strategy:

- Monitor newly created logon sessions

- Review authentication logs for abnormal credential usage

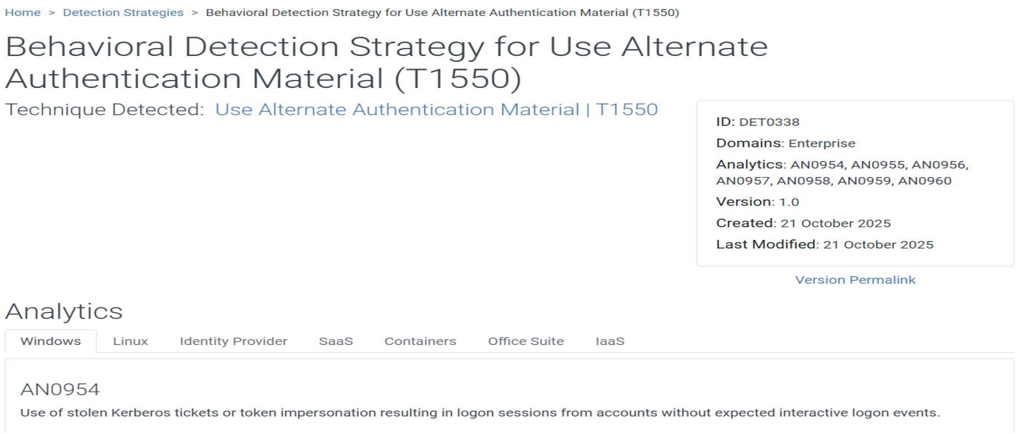
- Correlate logon source IPs with user behavior baselines

- Detect repeated authentication attempts across multiple systems using the same hash

MITRE Mapping:

Technique: T1550.002 (Use Alternate Authentication Material: Pass the Hash)

Tactic: Credential Access / Lateral Movement



Home > Detection Strategies > Behavioral Detection Strategy for Use Alternate Authentication Material (T1550)

Behavioral Detection Strategy for Use Alternate Authentication Material (T1550)

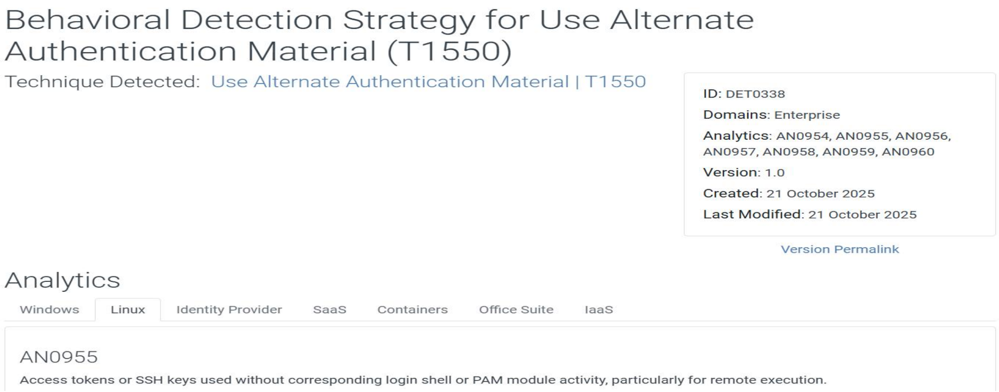
Technique Detected: Use Alternate Authentication Material | T1550

ID: DET0338
Domains: Enterprise
Analytics: AN0954, AN0955, AN0956, AN0957, AN0958, AN0959, AN0960
Version: 1.0
Created: 21 October 2025
Last Modified: 21 October 2025

Analytics

AN0954

Use of stolen Kerberos tickets or token impersonation resulting in logon sessions from accounts without expected interactive logon events.



Behavioral Detection Strategy for Use Alternate Authentication Material (T1550)

Technique Detected: Use Alternate Authentication Material | T1550

ID: DET0338
Domains: Enterprise
Analytics: AN0954, AN0955, AN0956, AN0957, AN0958, AN0959, AN0960
Version: 1.0
Created: 21 October 2025
Last Modified: 21 October 2025

Analytics

AN0955

Access tokens or SSH keys used without corresponding login shell or PAM module activity, particularly for remote execution.

5. MITRE Mapping Summary

Scenario	Tactic	Technique / ID
Cloud GUI Discovery	Discovery	T1538
Port 4050 C2 Traffic	Command and Control	G0099 (APT-C-36)
Network Entry Methods	Initial Access	TA001
Account Locking Malware	Impact	S0372 (LockerGoga)
Pass-the-Hash	Lateral Movement	T1550.002

6. Detection and Mitigation Strategies

- Enforce Multi-Factor Authentication (MFA) for all cloud and administrative accounts.

- Implement Conditional Access policies in Azure AD.

- Monitor cloud audit logs for excessive enumeration of users and roles.

- Block unnecessary outbound ports and inspect anomalous traffic patterns.

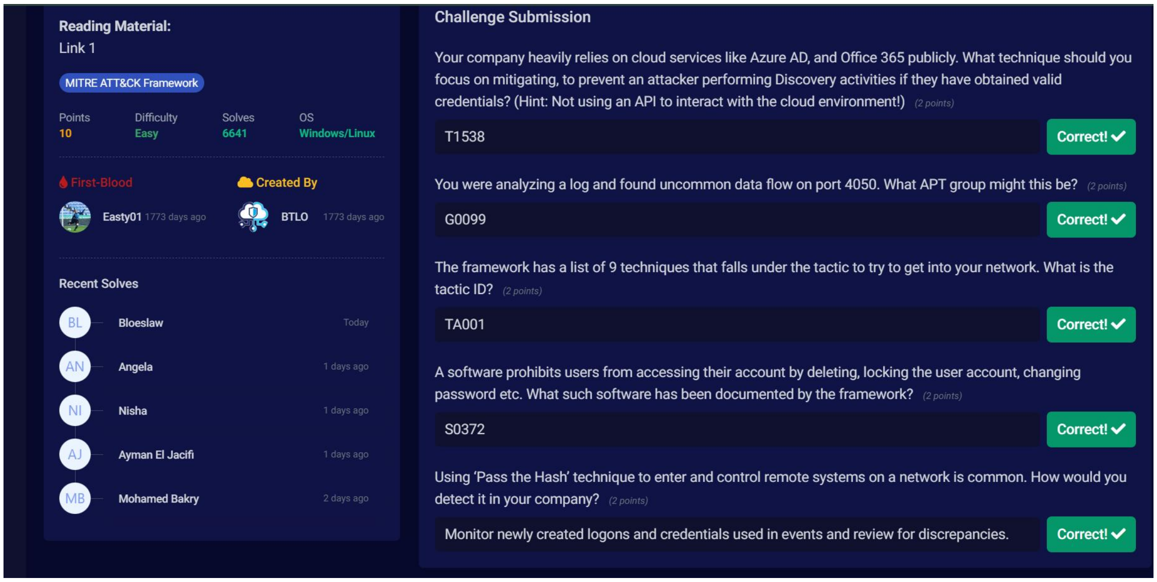
- Deploy Endpoint Detection and Response (EDR) solutions.

- Regularly rotate credentials and disable legacy authentication protocols.

- Conduct user awareness training on phishing and credential theft.

7. Final Verdict

This investigation demonstrates how the MITRE ATT&CK Framework can be operationalized to map real-world attack scenarios to documented adversary techniques and tactics. By leveraging threat intelligence, behavioral analysis, and proactive monitoring, organizations can improve detection capabilities and strengthen defenses against both opportunistic and advanced persistent threats. Continuous mapping of security events to the ATT&CK framework enables a structured and effective approach to enterprise and cloud security operations.



Reading Material:
Link 1

MITRE ATT&CK Framework

Points	Difficulty	Solves	OS
10	Easy	6641	Windows/Linux

First-Blood: Easty01 1773 days ago
Created By: BTLO 1773 days ago

Recent Solves

BL	Bloeslaw	Today
AN	Angela	1 days ago
NI	Nisha	1 days ago
AJ	Ayman El Jacifi	1 days ago
MB	Mohamed Bakry	2 days ago

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)

T1538 — Correct! ✓

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

G0099 — Correct! ✓

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)

TA001 — Correct! ✓

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)

S0372 — Correct! ✓

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)

Monitor newly created logons and credentials used in events and review for discrepancies. — Correct! ✓