To: Security Operations Center (SOC) Management

From: Ahmed Emad Nasr, SOC Analyst

Date: March 17, 2026

Subject: Cyber Threat Intelligence Brief – Cloud Migration & Aviation Sector Threats

1. Executive Summary

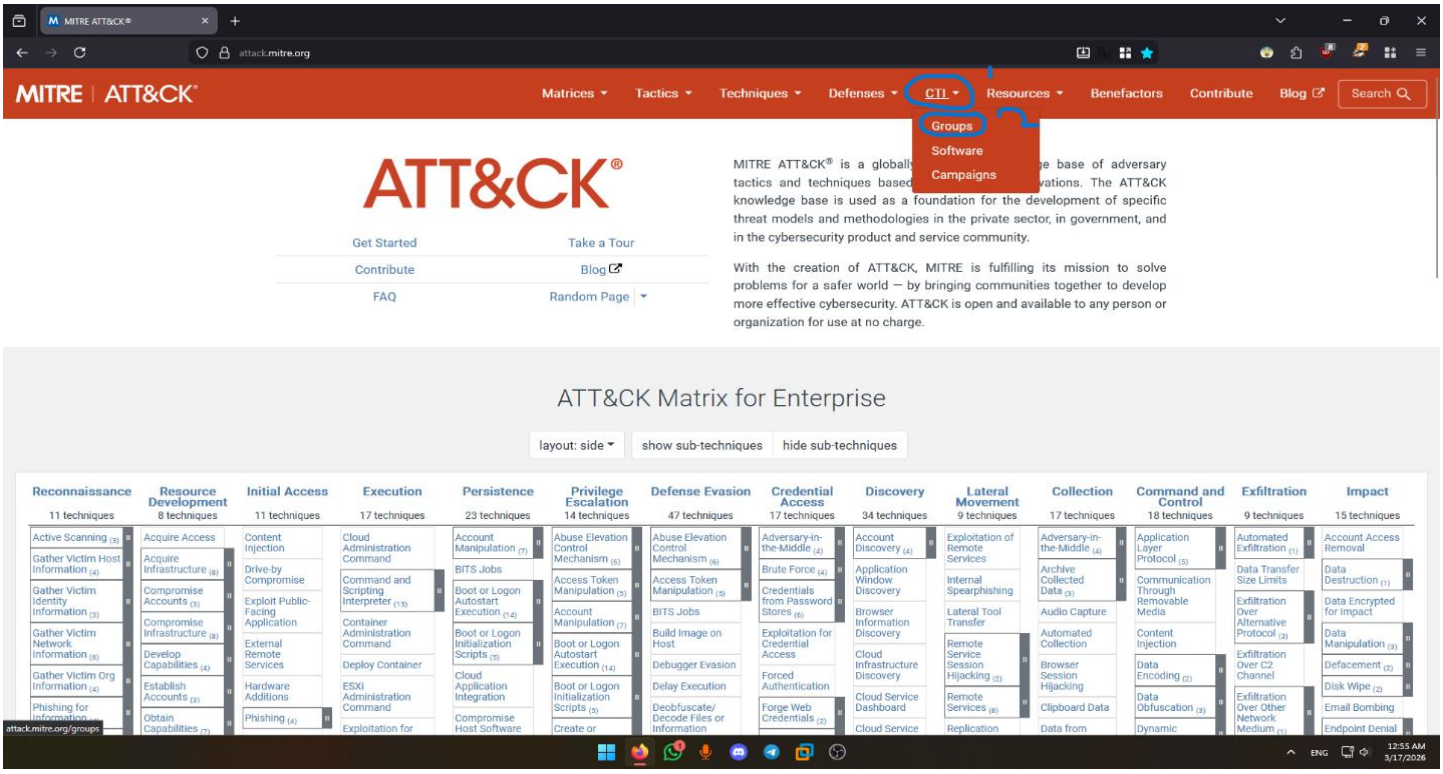
As our organization in the aviation sector transitions its infrastructure to the cloud, it is critical to assess the specific threat landscape associated with this environment. This intelligence brief identifies a primary Advanced Persistent Threat (APT) group known to target our sector, highlights their relevant tactics and tools, and outlines actionable defensive strategies to secure our Office 365 and cloud integrations.

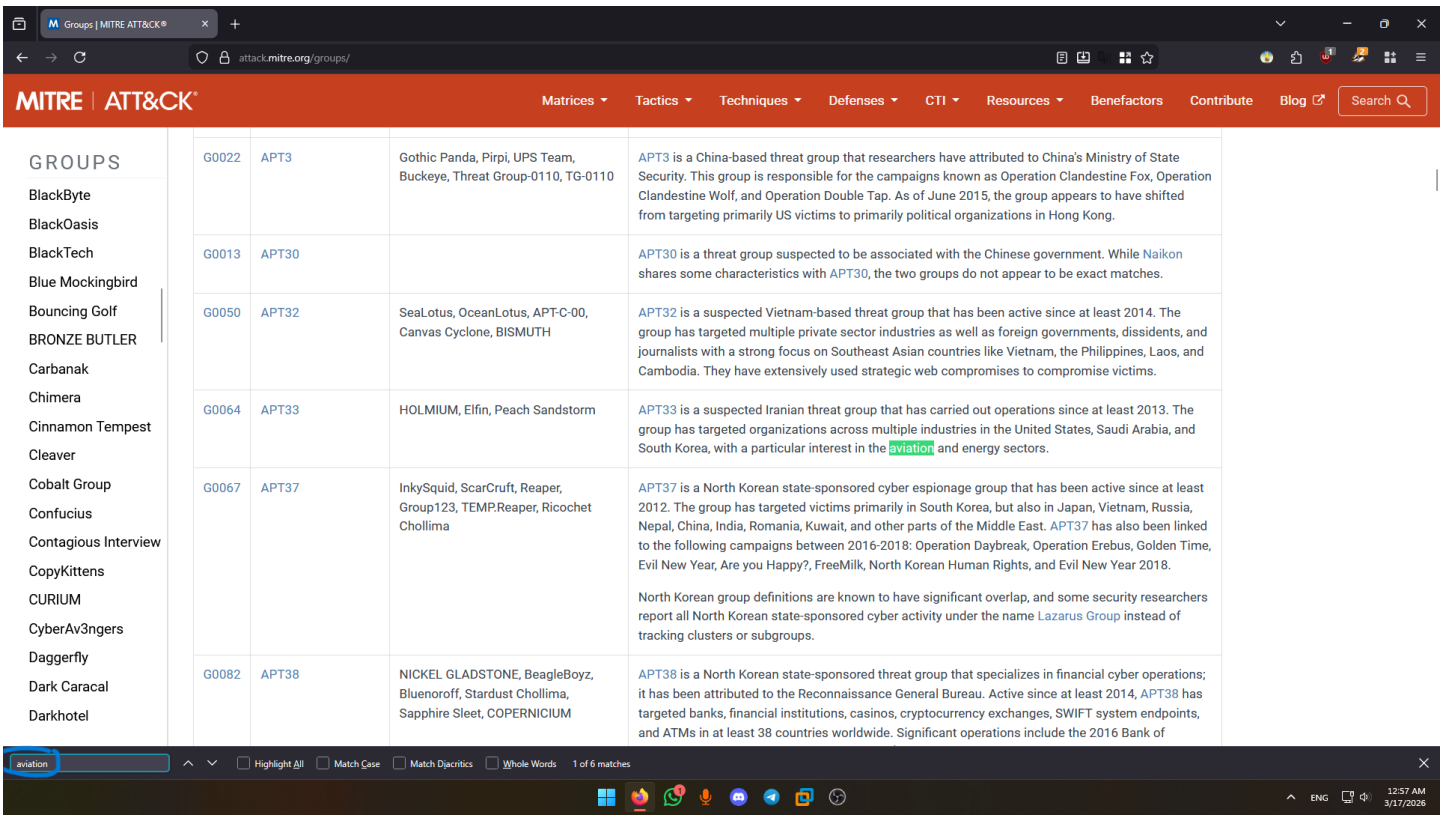
2. Threat Actor Profile

*** Threat Group: APT33**

*** Activity: Active since at least 2013.**

*** Target Profile: This group has a documented history of conducting operations against organizations across multiple industries, with a distinct and particular interest in the aviation and energy sectors.**

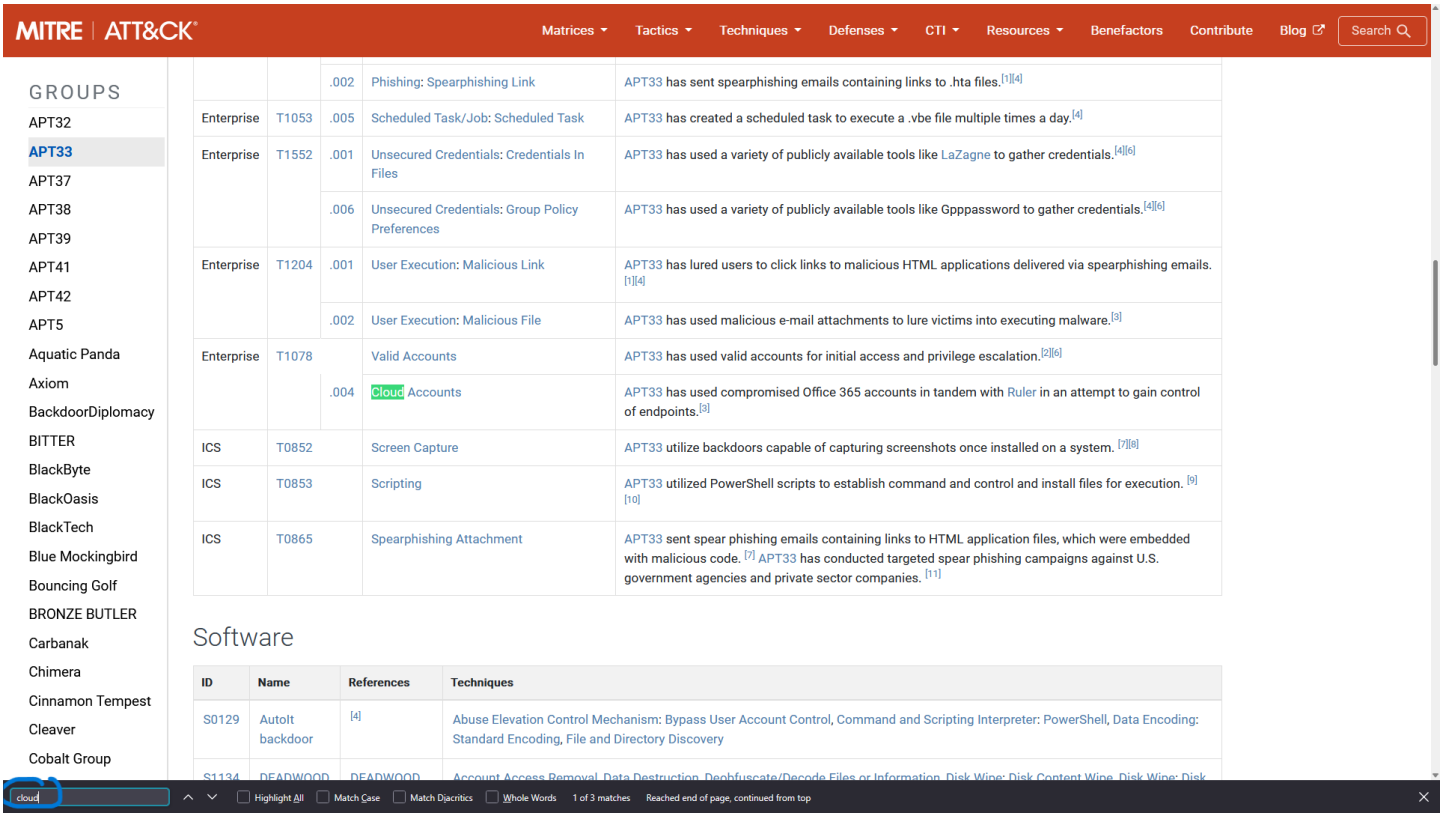

MITRE ATT&CK®
attack.mitre.org
MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Contribute
Blog
Search
Groups
Software
Campaigns
ATT&CK®
Get Started
Take a Tour
Contribute
Blog
FAQ
Random Page
MITRE ATT&CK® is a global
base of adversary tactics and techniques based
vations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
11 techniques
Resource Development
8 techniques
Initial Access
11 techniques
Execution
17 techniques
Persistence
23 techniques
Privilege Escalation
14 techniques
Defense Evasion
47 techniques
Credential Access
17 techniques
Discovery
34 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
18 techniques
Exfiltration
9 techniques
Impact
15 techniques
attack.mitre.org/groups


Groups | MITRE ATT&CK®
attack.mitre.org/groups/
MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Contribute
Blog
Search
GROUPS
BlackByte
BlackOasis
BlackTech
Blue Mockingbird
Bouncing Golf
BRONZE BUTLER
Carbanak
Chimera
Cinnamon Tempest
Cleaver
Cobalt Group
Confucius
Contagious Interview
CopyKittens
CURIUM
CyberAv3ngers
Daggerfly
Dark Caracal
Darkhotel
G0022 APT3 Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110 APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.
G0013 APT30 APT30 is a threat group suspected to be associated with the Chinese government. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.
G0050 APT32 SeaLotus, OceanLotus, APT-C-00, Canvas Cyclone, BISMUTH APT32 is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.
G0064 APT33 HOLMIUM, Elfin, Peach Sandstorm APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.
G0067 APT37 InkySquid, ScarCruft, Reaper, Group123, TEMP.Reaper, Ricochet Chollima APT37 is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. APT37 has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are you Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.
North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.
G0082 APT38 NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima, Sapphire Sleet, COPERNICIUM APT38 is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau. Active since at least 2014, APT38 has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of
aviation
Highlight All
Match Case
Match Diacritics
Whole Words
1 of 6 matches

3. Key Tactics, Techniques, and Procedures (TTPs)

*** Primary Sub-technique: Cloud Accounts (T1078.004)**

*** Context & Tooling: APT33 frequently targets cloud infrastructure, specifically focusing on Microsoft Office 365. The group utilizes compromised Office 365 accounts in tandem with a publicly available post-exploitation tool called Ruler to attempt to gain remote control over corporate endpoints.**



4. Defensive Recommendations

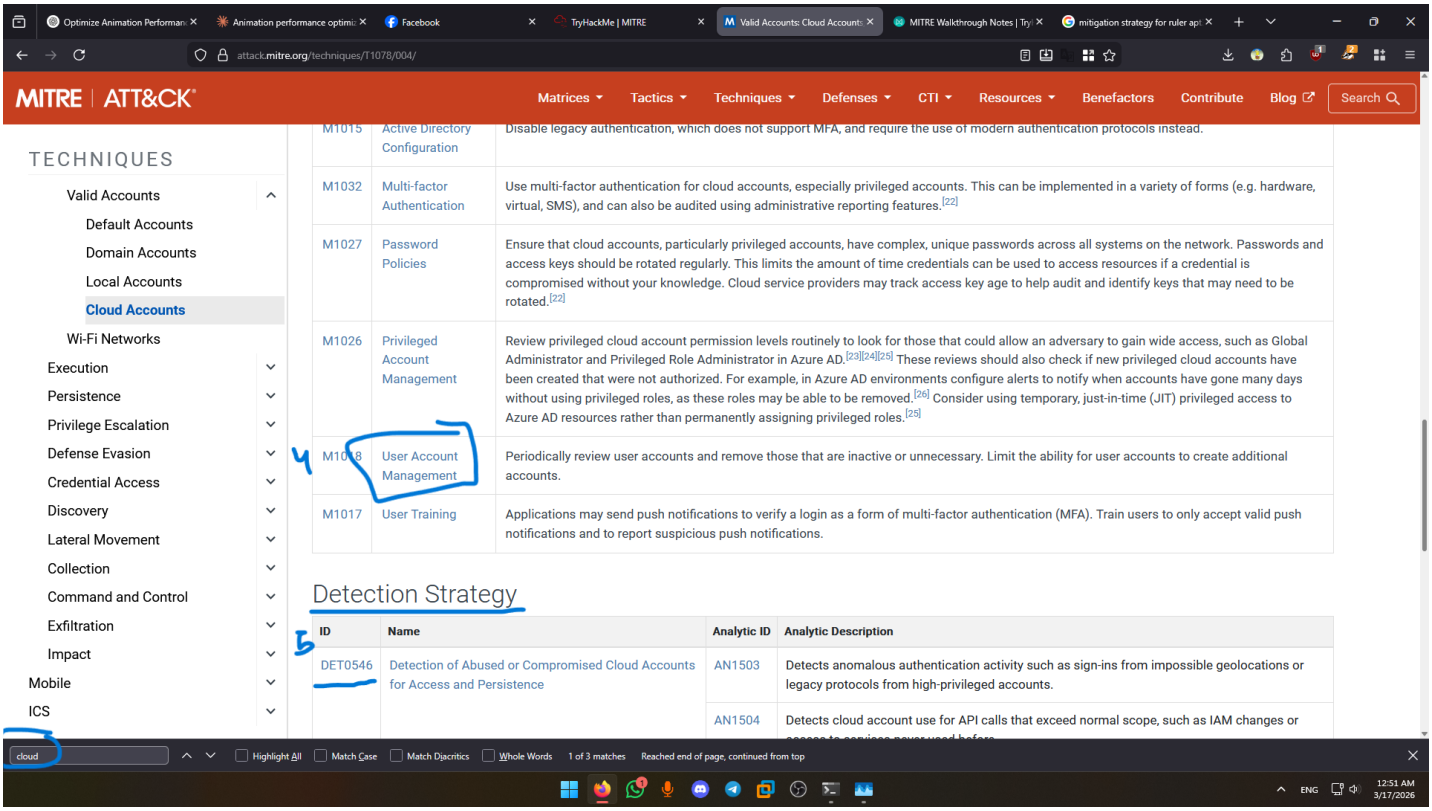
To address potential gaps in our defensive coverage during the cloud migration, the following mitigation and detection strategies must be prioritized:

*** Mitigation Strategy: Implement User Account Management (M1018).**

- Action: We must enforce a policy to periodically review all user accounts and immediately remove or disable those that are inactive, orphaned, or unnecessary. This directly reduces the attack surface for the Cloud Accounts technique.

*** Detection Strategy: Implement Detection Strategy DET0546.**

- Action: Deploy monitoring rules mapped to DET0546 to actively identify the "Detection of Abused or Compromised Cloud Accounts for Access and Persistence." This will help the SOC quickly catch anomalous authentication activity or API calls that exceed normal scope.



5. Conclusion

Securing our Office 365 environment against unauthorized access is a high priority. By strictly managing account lifecycles (M1018) and configuring our SIEM to detect compromised cloud account behavior (DET0546), we can significantly reduce the risk posed by adversaries like APT33.