

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®

Matrices | Tactics | Techniques | Defenses | **CTI** | Resources | Benefactors | Contribute | Blog | Search

ATT&CK®

Get Started | Take a Tour

Contribute | Blog

FAQ | Random Page

MITRE ATT&CK® is a global knowledge base of adversary tactics and techniques based on open source information. 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	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (2)	Acquire Access (1)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Exploitation of Remote Services (1)	Adversary-in-the-Middle (4)	Application Layer Protocol (3)	Automated Exfiltration (1)	Account Access Removal (1)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise (1)	Command and Scripting Interpreter (13)	BITS Jobs (1)	Access Token Manipulation (3)	Access Token Manipulation (3)	Access Token Manipulation (3)	Application Window Discovery (1)	Internal Spearphishing (1)	Archive Collected Data (3)	Communication Through Removable Media (1)	Data Transfer Size Limits (1)	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application (1)	Container Administration Command (1)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Account Manipulation (7)	Account Manipulation (7)	Browser Information Discovery (1)	Lateral Tool Transfer (1)	Audio Capture (1)	Content Injection (1)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact (1)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services (1)	Deploy Container (1)	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Cloud Infrastructure Discovery (1)	Remote Service Session Hijacking (2)	Automated Collection (1)	Browser Session Hijacking (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions (1)	ESXi Administration Command (1)	Cloud Application Integration (1)	Boot or Logon Initialization Scripts (3)	Debugger Evasion (1)	Debugger Evasion (1)	Cloud Service Dashboard (1)	Remote Services (3)	Clipboard Data (1)	Data Encoding (2)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (1)	Establish Accounts (3)	Phishing (4)	Exploitation for (1)	Compromise Host Software (1)	Create or (1)	Delay Execution (1)	Delay Execution (1)	Cloud Service (1)	Replication (1)	Data from (1)	Data Obfuscation (3)	Email Bombing (1)	Disk Wipe (2)
Obtain Capabilities (7)						Deobfuscate/Decode Files or Information (1)	Deobfuscate/Decode Files or Information (1)	Forge Web Credentials (2)			Dynamic (1)	Endpoint Denial (1)	

Groups | MITRE ATT&CK®

Matrices | Tactics | Techniques | Defenses | **CTI** | Resources | Benefactors | Contribute | Blog | Search

GROUPS	Group ID	APT	Group Name	Description
BlackByte	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.
BlackOasis	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.
BlackTech	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.
Blue Mockingbird	G0064	APT33	HOLMIUM, Eifn, 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.
Bouncing Golf	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.
BRONZE BUTLER	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 | 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.**

The screenshot shows the MITRE ATT&CK website interface. At the top, there is a navigation bar with links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, Contribute, and Blog. A search bar is located on the right side of the navigation bar. Below the navigation bar, there is a sidebar on the left labeled 'GROUPS' with a list of groups including APT32, APT33 (highlighted), APT37, APT38, APT39, APT41, APT42, APT5, Aquatic Panda, Axiom, BackdoorDiplomacy, BITTER, BlackByte, BlackOasis, BlackTech, Blue Mockingbird, Bouncing Golf, BRONZE BUTLER, Carbanak, Chimera, Cinnamon Tempest, Cleaver, and Cobalt Group. The main content area displays search results for the term 'cloud'. The results are organized into a table with columns for ID, Name, References, and Techniques. The first result is for T1078.004, 'Cloud Accounts', which is highlighted in green. The description for this technique states: 'APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints.' Below the table, there is a 'Software' section with a table of software entries. The first entry is S0129, 'Autolt backdoor', with a reference to [4] and a description: 'Abuse Elevation Control Mechanism: Bypass User Account Control, Command and Scripting Interpreter: PowerShell, Data Encoding: Standard Encoding, File and Directory Discovery'. At the bottom of the screenshot, there is a search bar with the word 'cloud' entered and a search button. Below the search bar, there are search options: Highlight All, Match Case, Match Diacritics, and Whole Words. The search results show 1 of 3 matches and a note that the search reached the end of the page, continuing from the top.

ID	Name	References	Techniques
S0129	Autolt backdoor	[4]	Abuse Elevation Control Mechanism: Bypass User Account Control, Command and Scripting Interpreter: PowerShell, Data Encoding: Standard Encoding, File and Directory Discovery
S1134	DEADWOOD	DEADWOOD	Account Access Removal, Data Destruction, Deny/Restrict/Decode Files or Information, Disk Wipe: Disk Content Wipe, Disk Wipe: Disk

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.

The screenshot shows the MITRE ATT&CK website. On the left, a navigation menu lists various categories, with 'Cloud Accounts' highlighted. The main content area displays a table of techniques. The 'User Account Management' technique (M1018) is circled in blue. Below this, the 'Detection Strategy' section is visible, featuring a table with the following data:

ID	Name	Analytic ID	Analytic Description
DET0546	Detection of Abused or Compromised Cloud Accounts for Access and Persistence	AN1503	Detects anomalous authentication activity such as sign-ins from impossible geolocations or legacy protocols from high-privileged accounts.
		AN1504	Detects cloud account use for API calls that exceed normal scope, such as IAM changes or access to sensitive resources before...

At the bottom of the page, a search bar contains the word 'cloud', and a status bar indicates '1 of 3 matches'.

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.