Proof of Concept (PoC) – Cloud Storage Threat Matrix

Prepared By: Sandhya Singh

Intern ID: 233

1. Reconnaissance (TA0043)

Attacker's goal: Gather information about cloud storage resources before attacking.

Technique 1: Cloud Storage Object Discovery (T1619)

- **P1:** aws s3 ls or az storage blob list lists all available storage buckets/blobs. This tells the attacker what's available to target.
- **P2:** Query storage metadata APIs to get object creation dates, permissions, and other properties — helps in identifying old/unused assets to exploit.

Technique 2: Search Open Cloud Storage (T1593.003)

- **P1:** Use **Google Dorking** to find public S3 bucket URLs, Azure blobs, or GCP storage endpoints.
- **P2:** Use scanning tools like **S3Scanner** to locate open, misconfigured storage.

Technique 3: Cloud Account Enumeration (T1087.004)

- **P1:** Look for account aliases in public GitHub repos or forum posts.
- **P2:** Use WHOIS/cloud provider APIs to extract more account details.

Why important:
Recon helps attackers **map the environment** and identify entry points **without touching the target directly**, minimizing detection risk.

2. Resource Development (TA0042)

Attacker's goal: Prepare the tools, accounts, and infrastructure for the attack.

Technique 1: Acquire Cloud Infrastructure (T1583.003)

- **P1:** Create an attacker-owned bucket to store stolen data.
- **P2:** Enable public access so malware/C2 traffic can come and go easily.

Technique 2: Obtain Cloud Credentials (T1589.003)

- **P1:** Buy stolen keys on the dark web.
- **P2:** Harvest API tokens from exposed config files.

Technique 3: Setup Cloud-Based C2 Infrastructure (T1584.004)

- **P1:** Host malicious files in a bucket.
- **P2:** Use signed URLs to send instructions to malware without being blocked by firewalls.

Why important:
This stage **sets the stage for intrusion** — infrastructure is ready before the actual attack begins.

3. Initial Access (TA0001)

Attacker's goal: Get into the target's cloud storage environment.

Technique 1: Valid Accounts – Cloud Accounts (T1078.004)

- **P1:** Use leaked credentials from breaches.
- **P2:** Use hardcoded API keys found in source code.

Technique 2: Exploit Public-Facing Cloud Applications (T1190)

- **P1:** Exploit misconfigured storage interfaces.
- **P2:** Upload files that exploit vulnerabilities in server processing.

Technique 3: Supply Chain Compromise – Cloud Services (T1195.003)

- **P1:** Inject malicious files into shared cloud folders.
- **P2:** Modify scripts hosted in shared environments to infect users.

Why important:
Initial access is **the door-opening step** — if this fails, the rest of the attack can't happen.

4. Execution (TA0002)

Attacker's goal: Run malicious code or commands.

Technique 1: Command-Line Interface (T1059.004)

- **P1:** Use CLI tools to download files.
- **P2:** Automate large transfers with sync commands.

Technique 2: Cloud API Execution (T1106)

- **P1:** Call GetObject to fetch sensitive files.
- **P2:** Call PutObject to upload scripts for execution later.

Technique 3: User Execution – Malicious File (T1204.002)

- **P1:** Host a malicious doc and send link to victim.
- **P2:** Malware executes when victim opens the file.

Why important:
Execution moves the attack from **passive observation** to **active compromise**.

5. Persistence (TA0003)

Attacker's goal: Keep access even if discovered.

Technique 1: Add Cloud Access Keys (T1098.003)

- **P1:** Create extra API keys.
- **P2:** Spread them across regions.

Technique 2: Modify Cloud Storage Lifecycle Policies (T1098)

- **P1:** Prevent deletion of attacker's files.
- **P2:** Replicate them across multiple buckets.

Technique 3: Deploy Cloud Storage Backdoor (Custom)

- **P1:** Insert malicious code in static files.
- **P2:** Use it to regain access if blocked.

Why important:
Persistence ensures **long-term infiltration**, useful for espionage or continuous data theft.

6. Privilege Escalation (TA0004)

Attacker's goal: Increase access rights.

Technique 1: Modify Cloud IAM Policies (T1098.003)

- **P1:** Grant admin roles to attacker accounts.
- **P2:** Add wildcard permissions.

Technique 2: Exploit Misconfigured Trust Policies (T1484.002)

- **P1:** Assume roles with higher privileges.
- **P2:** Chain trust rules to escalate.

Technique 3: Cloud API Abuse for Escalation (T1610)

- **P1:** Exploit API version flaws.
- **P2:** Use old API endpoints to bypass restrictions.

Why important:
Escalation turns **basic access into full control**.

7. Defense Evasion (TA0005)

Attacker's goal: Avoid being detected.

Technique 1: Modify Cloud Storage Permissions (T1562.003)

- **P1:** Disable logging.
- **P2:** Change ACLs to hide activities.

Technique 2: Encrypt Data for Obfuscation (T1027)

- **P1:** Store stolen files in encrypted form.
- **P2:** Use uncommon compression to evade scanners.

Technique 3: Timestamp Manipulation (T1070.006)

- **P1:** Change file dates.
- **P2:** Fake creation times.

Why important:
Without evasion, defenders can **spot suspicious activity** quickly.

8. Credential Access (TA0006)

Attacker's goal: Steal cloud credentials.

Technique 1: Cloud Credentials in Files (T1552.005)

- **P1:** Search .env files for keys.
- **P2:** Scan build artifacts for tokens.

Technique 2: Access Key Logging (T1556)

- **P1:** Alter function logs to capture API calls.
- **P2:** Store them in attacker's bucket.

Technique 3: Steal Browser-Based Cloud Session Tokens (T1539)

- **P1:** Phish for admin cookies.
- **P2:** Replay them to log in.

Why important:
Credential theft can **bypass MFA** and allow silent login.

9. Discovery (TA0007)

Attacker's goal: Learn about the environment.

Technique 1: Permission Group Discovery – Cloud Storage (T1069.003)

- **P1:** List IAM groups with storage access.
- **P2:** Identify members.

Technique 2: Storage Region Discovery (T1590.004)

- **P1:** Find where buckets are hosted.
- **P2:** Map replication.

Technique 3: File Type Discovery (T1083)

- **P1:** Search for sensitive file types.
- **P2:** Locate backups.

10. Lateral Movement (TA0008)

Attacker's goal: Move to other accounts/projects.

Technique 1: Cloud Service Account Impersonation (T1538)

- **P1:** Act as another account.
- **P2:** Access other files.

Technique 2: Cross-Account Bucket Access (Custom)

- **P1:** Use shared permissions.
- **P2:** Plant malicious files.

Technique 3: Cloud Storage Sync Abuse (T1021)

- **P1:** Sync victim's data to attacker bucket.
- **P2:** Keep bidirectional sync.

11. Collection (TA0009)

Attacker's goal: Gather data for theft.

Technique 1: Archive Collected Data (T1560)

- **P1:** Compress before theft.
- **P2:** Split into smaller files.

Technique 2: Cloud Storage Data Staging (T1074.002)

- **P1:** Store stolen data temporarily.
- **P2:** Hide it with harmless tags.

Technique 3: Screen Capture Storage (T1113)

- **P1:** Save screenshots.
- **P2:** Encrypt before upload.

12. Command and Control (TA0011)

Attacker's goal: Control malware remotely.

Technique 1: Web Service (T1102)

- **P1:** Store config in cloud blobs.
- **P2:** Retrieve updates via URLs.

Technique 2: Exfiltration Channel via Storage (T1567.002)

- **P1:** Upload stolen data as beacon.
- **P2:** Read commands from cloud.

Technique 3: Dead Drop Resolver (T1102.001)

- **P1:** Hide commands in public files.
- **P2:** Use versioning for updates.

13. Exfiltration (TA0010)

Attacker's goal: Steal data.

Technique 1: Exfiltration to Cloud Storage (T1567.002)

- **P1:** Upload stolen data to attacker bucket.
- **P2:** Use multipart uploads.

Technique 2: Data Transfer Size Limits Bypass (T1030)

- **P1:** Split files.
- **P2:** Use parallel uploads.

Technique 3: Scheduled Exfiltration (T1029)

- **P1:** Upload during low-traffic times.
- **P2:** Automate with triggers.

14. Impact (TA0040)

Attacker's goal: Cause damage.

Technique 1: Data Destruction – Cloud Storage (T1485)

- **P1:** Delete all files.
- **P2:** Overwrite with zero-byte files.

Technique 2: Resource Hijacking (T1496)

- **P1:** Host illegal content.
- **P2:** Host crypto miners.

Technique 3: Defacement – Cloud Content (T1491.001)

- **P1:** Replace web assets.
- **P2:** Display attacker's message.