# Proof of Concept (PoC) – Cloud Storage Threat Matrix

Prepared By: Sandhya Singh

Intern ID: 233

Proof of Concept (PoC) – Cloud Storage Threat Matrix

Task Title: Cloud Storage Security Simulation (Microsoft Threat Matrix)

Prepared By: [Sandhya Singh]]

Inern ID : 233

1. Reconnaissance (TA0043)

Technique 1: Cloud Storage Object Discovery (T1619)

Procedure 1 : Use aws s3 ls or az storage blob list to enumerate available buckets/blobs.

Procedure 2 : Query storage metadata APIs to collect object creation dates and permissions.

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

Procedure 1 : Use Google Dorking to find public cloud storage URLs.

Procedure 2 : Scan for open S3 buckets with tools like S3Scanner.

Technique 3: Cloud Account Enumeration (T1087.004)

Procedure 1 : Identify cloud account aliases from public repositories.

Procedure 2 : Enumerate account details via WHOIS and cloud provider APIs.

2. Resource Development (TA0042)

Technique 1: Acquire Cloud Infrastructure (T1583.003)

Procedure 1 : Create an attacker-controlled cloud bucket for staging stolen data.

Procedure 2 : Enable public access for easy inbound/outbound data flow.

Technique 2: Obtain Cloud Credentials (T1589.003)

Procedure 1: Purchase stolen cloud keys from dark web markets.

P2: Harvest API tokens from leaked configuration files.

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

P1: Host malicious payloads in a cloud storage bucket.

P2: Configure signed URLs to deliver C2 instructions to infected clients.

3. Initial Access (TA0001)

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

P1: Use leaked cloud credentials from a data breach.

P2: Use hardcoded API keys from application source code.

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

P1: Exploit misconfigured storage web interfaces to gain access.

P2: Upload a malicious file to trigger server-side vulnerabilities.

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

P1: Inject malicious files into a shared storage used by multiple tenants.

P2: Alter shared cloud-hosted scripts to gain execution in victim environments.

---

4. Execution (TA0002)

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

P1: Execute aws s3 cp to copy files from storage.

P2: Automate repeated sync commands for large-scale transfers.

Technique 2: Cloud API Execution (T1106)

P1: Invoke GetObject API calls to download sensitive files.

P2: Use PutObject to upload scripts for later execution.

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

P1: Host a malicious document in storage and send the link to a target.

P2: Trigger execution when the target downloads and opens the file.

---

5. Persistence (TA0003)

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

P1: Create secondary API keys for an existing account.

P2: Store keys in multiple cloud regions to ensure redundancy.

Technique 2: Modify Cloud Storage Lifecycle Policies (T1098)

P1: Change retention rules to prevent deletion of attacker files.

P2: Auto-replicate attacker files to multiple buckets.

Technique 3: Deploy Cloud Storage Backdoor (Custom)

P1: Embed malicious code in cloud-hosted static files.

P2: Use the backdoor to re-establish access if main credentials are revoked.

---

6. Privilege Escalation (TA0004)

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

P1: Assign “Storage Admin” role to attacker-controlled accounts.

P2: Add wide wildcard permissions (s3:\*) to own account.

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

P1: Assume privileged roles from misconfigured storage policies.

P2: Chain trust policies to escalate access rights.

Technique 3: Cloud API Abuse for Escalation (T1610)

P1: Exploit API version mismatches to bypass permission checks.

P2: Abuse legacy API endpoints for elevated access.

---

7. Defense Evasion (TA0005)

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

P1: Remove logging and auditing from buckets.

P2: Change ACLs to prevent activity tracking.

Technique 2: Encrypt Data for Obfuscation (T1027)

P1: Store stolen files in encrypted archives.

P2: Use uncommon compression formats to evade detection.

Technique 3: Timestamp Manipulation (T1070.006)

P1: Alter object metadata to hide recent changes.

P2: Fake object creation dates to mislead investigators.

---

8. Credential Access (TA0006)

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

P1: Search .env files for storage keys.

P2: Scan build artifacts for embedded tokens.

Technique 2: Access Key Logging (T1556)

P1: Modify cloud function logs to capture API calls.

P2: Store logged keys in attacker-controlled storage.

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

P1: Use phishing to obtain storage admin session cookies.

P2: Replay cookies to authenticate into cloud console.

---

9. Discovery (TA0007)

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

P1: List IAM groups with storage privileges.

P2: Identify user accounts in those groups.

Technique 2: Storage Region Discovery (T1590.004)

P1: Identify where storage buckets are hosted.

P2: Map cross-region replication for data movement.

Technique 3: File Type Discovery (T1083)

P1: Search storage for .pdf or .docx sensitive files.

P2: Identify backup archives and database dumps.

---

10. Lateral Movement (TA0008)

Technique 1: Cloud Service Account Impersonation (T1538)

P1: Assume identity of another account with storage privileges.

P2: Access files belonging to different projects.

Technique 2: Cross-Account Bucket Access (Custom)

P1: Use shared bucket permissions to move into another tenant’s environment.

P2: Upload malicious files to shared collaboration buckets.

Technique 3: Cloud Storage Sync Abuse (T1021)

P1: Sync from victim’s bucket to attacker’s bucket.

P2: Set up bidirectional sync to maintain continuous access.

---

11. Collection (TA0009)

Technique 1: Archive Collected Data (T1560)

P1: Compress sensitive data before exfiltration.

P2: Split large files into multiple chunks to avoid detection.

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

P1: Store staged files in temporary buckets.

P2: Tag staged files with harmless labels to avoid suspicion.

Technique 3: Screen Capture Storage (T1113)

P1: Store screenshots from compromised systems in cloud storage.

P2: Encrypt screenshots before upload.

---

12. Command and Control (TA0011)

Technique 1: Web Service (T1102)

P1: Host C2 config in cloud storage blobs.

P2: Retrieve updates from public URLs.

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

P1: Upload beacon data to a controlled bucket.

P2: Poll storage URLs for C2 instructions.

Technique 3: Dead Drop Resolver (T1102.001)

P1: Store encoded commands in public files.

P2: Use file versioning to deliver new instructions without altering URLs.

---

13. Exfiltration (TA0010)

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

P1: Upload sensitive files to attacker-controlled buckets.

P2: Use multi-part uploads for large datasets.

Technique 2: Data Transfer Size Limits Bypass (T1030)

P1: Split files into smaller chunks.

P2: Use parallel uploads for speed.

Technique 3: Scheduled Exfiltration (T1029)

P1: Schedule uploads during low network usage times.

P2: Automate with cloud event triggers.

14. Impact (TA0040)

Technique 1: Data Destruction – Cloud Storage (T1485)

P1: Delete all objects in production buckets.

P2: Overwrite sensitive files with zero-byte objects.

Technique 2: Resource Hijacking (T1496)

P1: Use storage as illegal hosting for pirated content.

P2: Host cryptomining payloads in storage.

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

Procedure 1 : Replace website assets in storage with defaced versions.

Procedure 2 :Alter public files to display attacker messages.

2. Conclusion

This PoC maps all 14 MITRE ATT&CK tactics to 3 relevant cloud storage techniques each, with

2 detailed procedures per technique, totalling 84 actionable procedures. This structure enables

a realistic simulation of attacker activity in a cloud storage environment, from reconnaissance

through final impact.