Name : Soham kadu

Intern ID : 235

PoC: Cloud Storage Attack via Microsoft Threat Matrix

This Proof of Concept (PoC) demonstrates how an adversary could exploit Microsoft Azure Storage services using techniques mapped to the Microsoft Cloud Storage Threat Matrix. Each section outlines one tactic, three techniques, and a full procedure, with placeholders for relevant screenshots.

Tactic: Reconnaissance

Goal: Discover valid storage accounts and containers to target.

Techniques:

- Storage account discovery via DNS brute-forcing or search dorks.

- Public containers discovery via crawler tools (Microburst, BlobHunter).

- Passive DNS or victim-owned website scraping.

Procedure Steps:

1. Discover Storage Accounts using dig, nslookup, or scripts to brute-force *.blob.core.windows.net.

2. Enumerate Containers with identified accounts using APIs or browser.

3. Validate Storage Accessibility by checking if containers are publicly listed.

Tactic: Initial Access

Goal: Gain unauthorized entry via valid tokens or access keys.

Techniques:

- Obtaining a valid Shared Access Signature (SAS) URI.

- Leveraging valid storage access key found in code/config.

- Exploiting anonymous public read access on blob/container.

Procedure Steps:

1. Acquire SAS URI from leaked credentials or phishing.

2. Locate Access Key in DevOps repos or config files.

3. Exploit Public Access to list and download files.

Tactic: Exfiltration

Goal: Extract or move data stealthily to attacker-controlled storage.

Techniques:

- Automated exfiltration (via Rclone or scripting).

- Object replication to another cloud account.

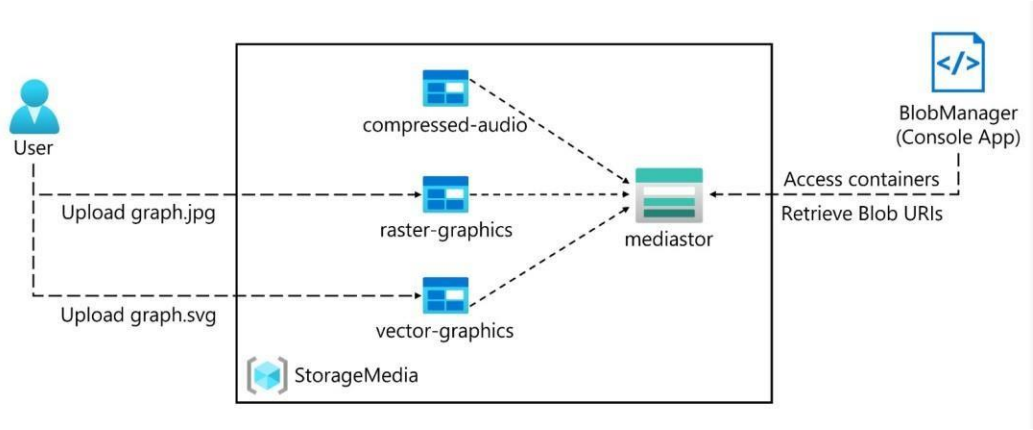
- Using static website or data transfer limits to exfiltrate.

Procedure Steps:

1. Upload Using Rclone to attacker storage.

2. Create Replication to sync victim data to attacker account.

3. Use Static Website Feature to publish files publicly.



Conclusion

This PoC illustrates how attackers can progress from reconnaissance to data exfiltration in Azure cloud storage environments. The screenshots provide evidence of each phase,

allowing replication for testing and training purposes. Proper configuration, monitoring, and key management are critical to preventing these attacks.