TASK: Threat Intelligence
Name: Vinit Chaskar
Intern ID: 395
Date: 29/07/2025
Tactic Chosen: Execution / Exfiltration (TA0002 / TA0010)
MITRE Link: https://attack.mitre.org/tactics/TA0002/

Description of the Tactic

The Execution and Exfiltration tactics involve techniques where attackers either execute malicious code or extract sensitive data from target environments.
In the context of **cloud storage**, attackers may abuse legitimate platform features like **object replication**, **static website hosting**, and **private endpoints** to execute commands, distribute malware, or exfiltrate sensitive data — often without triggering security alerts.

Execution in cloud storage can happen through legitimate admin tools, while exfiltration often uses overlooked or misconfigured features.

Objective of This PoC

To demonstrate how attackers can abuse cloud storage services for malicious purposes by leveraging three techniques:

- **Object Replication (Exfiltration & Malware Delivery)**
- **Static Website (Data Exfiltration)**
- **Private Endpoint (Defense Evasion & Persistence)**

□ Techniques Selected (with MITRE IDs)

Technique ID	Technique Name	MITRE Link
T1537	Transfer Data to Cloud Account (Object Replication)	https://attack.mitre.org/techniques/T1537/
T1567.002	Exfiltration to Cloud Storage (Static Website)	https://attack.mitre.org/techniques/T1567/002/
T1090.001	Proxy: Internal Proxy (Private Endpoint Abuse)	https://attack.mitre.org/techniques/T1090/001/