OH CR&P!
I think we've been breached

Applications of the MITRE ATT&CK framework on Google Cloud

Authors: Garrett Wong, Wilson Liu

Disclaimer

The following presentation is a representation of our own research and not necessarily the opinions of Google Cloud.

This presentation does not discuss forward looking statements, non-public material or confidential information.

The Presenters

Garrett Wong
Strategic Cloud Engineer

Wilson Liu
Strategic Cloud Engineer

MITRE ATT&CK Brief

The MITRE ATT&CK® framework is the most widely adopted investigation framework at present

Many enterprises are moving toward more widespread adoption as this framework improves its integration and automation capabilities.

Knowledge base of adversary tactics, techniques and procedures (TTPs).

63% Orgs use MITRE ATT&CK in their SOC [1]

81% Orgs experience ATT&CK techniques monthly [1]

87% Adopting ATT&CK for will improve security posture [1]

1. https://cltc.berkeley.edu/wp-content/uploads/2020/10/MITRE_ATTCK_Framework_Report.pdf

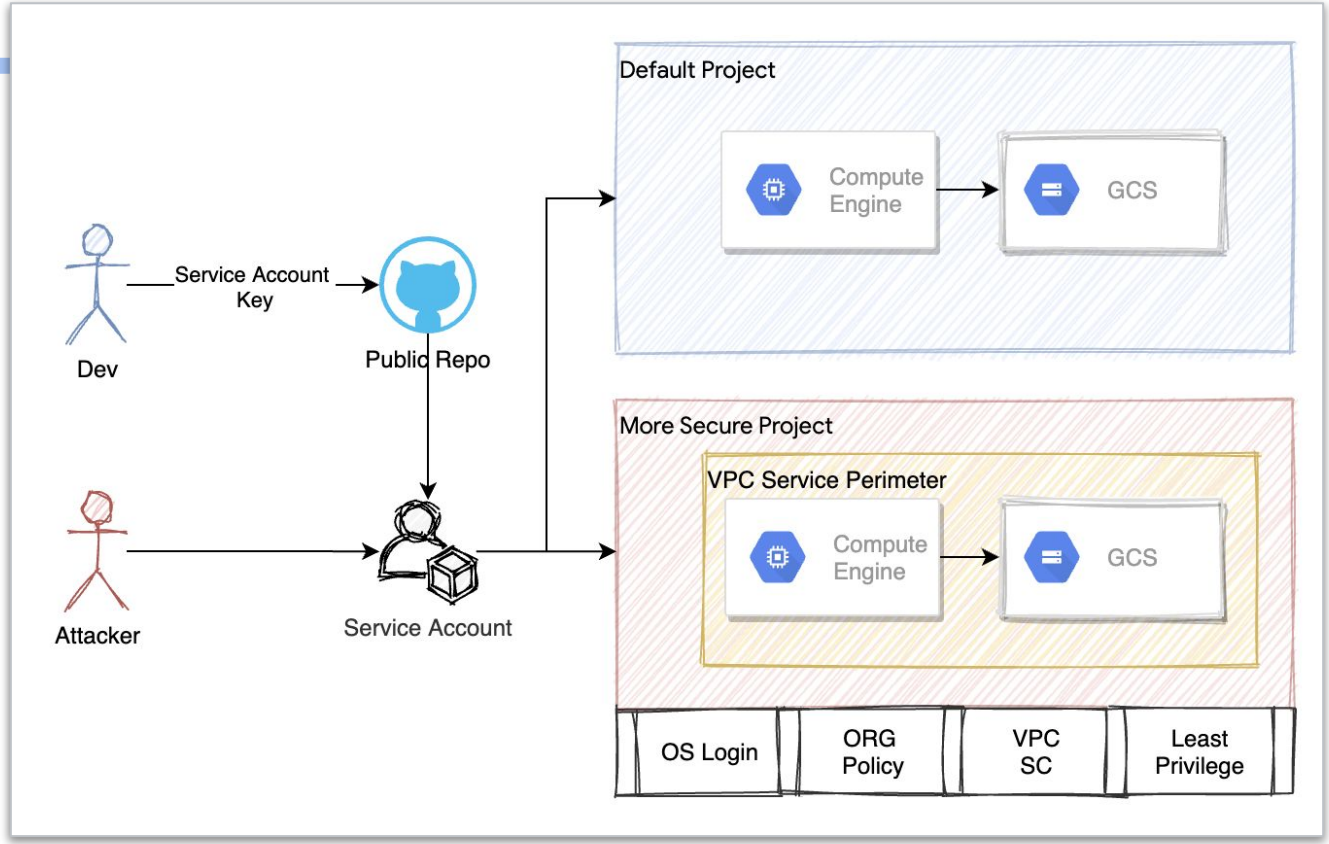
In this Presentation...

We'll introduce **2 Cloud Reference Architectures.** The **first** is representative of an unsecured, default GCP Project. The **second** will be a more secured GCP Project Environment.

We'll simulate, discuss and demonstrate the impacts of the **Leaked Credential event** from both a Red Team and Blue Team perspective.

We'll conclude with security best practices, recommendations around detective and preventive measures to bolster your **cloud security posture**.

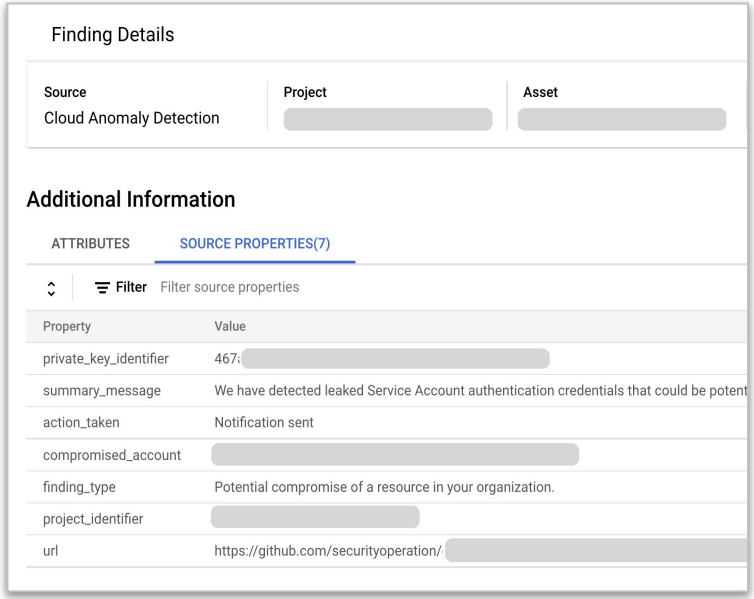
Architectures



The Incident

The Default Compute Service Account Key Uploaded to a Public Repository


```
{
"type": "service_account",
"project_id": "test-project",
"private_key_id": "c2b3338615862235b5d65992ee04aa3b6312a055",
"private_key": "-----BEGIN PRIVATE KEY-----\..w==\n-----END
PRIVATE KEY-----\n",
"client_email": "268323096253-
compute@developer.gserviceaccount.com",
"client_id": "111950642475515960564",
"auth_uri": "https://accounts.google.com/o/oauth2/auth",
"token_uri": "https://oauth2.googleapis.com/token",
"auth_provider_x509_cert_url":
"https://www.googleapis.com/oauth2/v1/certs",
"client_x509_cert_url":
"https://www.googleapis.com/robot/v1/metadata/x509/268323096253-
compute%40developer.gserviceaccount.com"
}
```

T1078

Initial Access

Valid Accounts

T1098

Persistence

Account Manipulation

T1537

Exfiltration

Transfer Data to Cloud Account

T1496

Impact

Resource Hijacking

Initial Access: Valid Accounts

Attack

```
gcloud auth activate-service-account --key-file
key.json

gcloud auth list

gcloud projects get-iam-policy $PROJECT_ID
```

Initial Access: Valid Accounts

Initial Attack

```
To set the active account, run:
    $ gcloud config set account `ACCOUNT`

att&ck $
att&ck $ gcloud projects list
PROJECT_ID     NAME           PROJECT_NUMBER
mitre-default  mitre-default  173814306518
att&ck $ gcloud projects get-iam-policy mitre-default
bindings:
- members:
  - serviceAccount:service-173814306518@compute-system.iam.gserviceaccount.com
  role: roles/compute.serviceAgent
- members:
  - serviceAccount:173814306518-compute@developer.gserviceaccount.com
  - serviceAccount:173814306518@cloudservices.gserviceaccount.com
  role: roles/editor
- members:
  - serviceAccount:service-173814306518@gcp-sa-websecurityscanner.iam.gserviceac
count.com
  role: roles/websecurityscanner.serviceAgent
etag: BwXLD3W3Pz4=
version: 1
```

Initial Access: Valid Accounts

Detect | Mitigate

Detect Threat

- Anomaly Detection Leaked Credentials (SCC Finding)
- SA Self Investigation Alert (SCC Findings)
- Suspicious IPs (Admin Activity logs)

Mitigate Threat

- Disable Auto IAM Grants for Default Accounts
- Disable service account key creation
- Workload Identity Federation
- VPC Service Controls

Initial Access: Valid Accounts

Mitigate the Attack

Persistence: Account Manipulation

Attack

Create SSH Keys

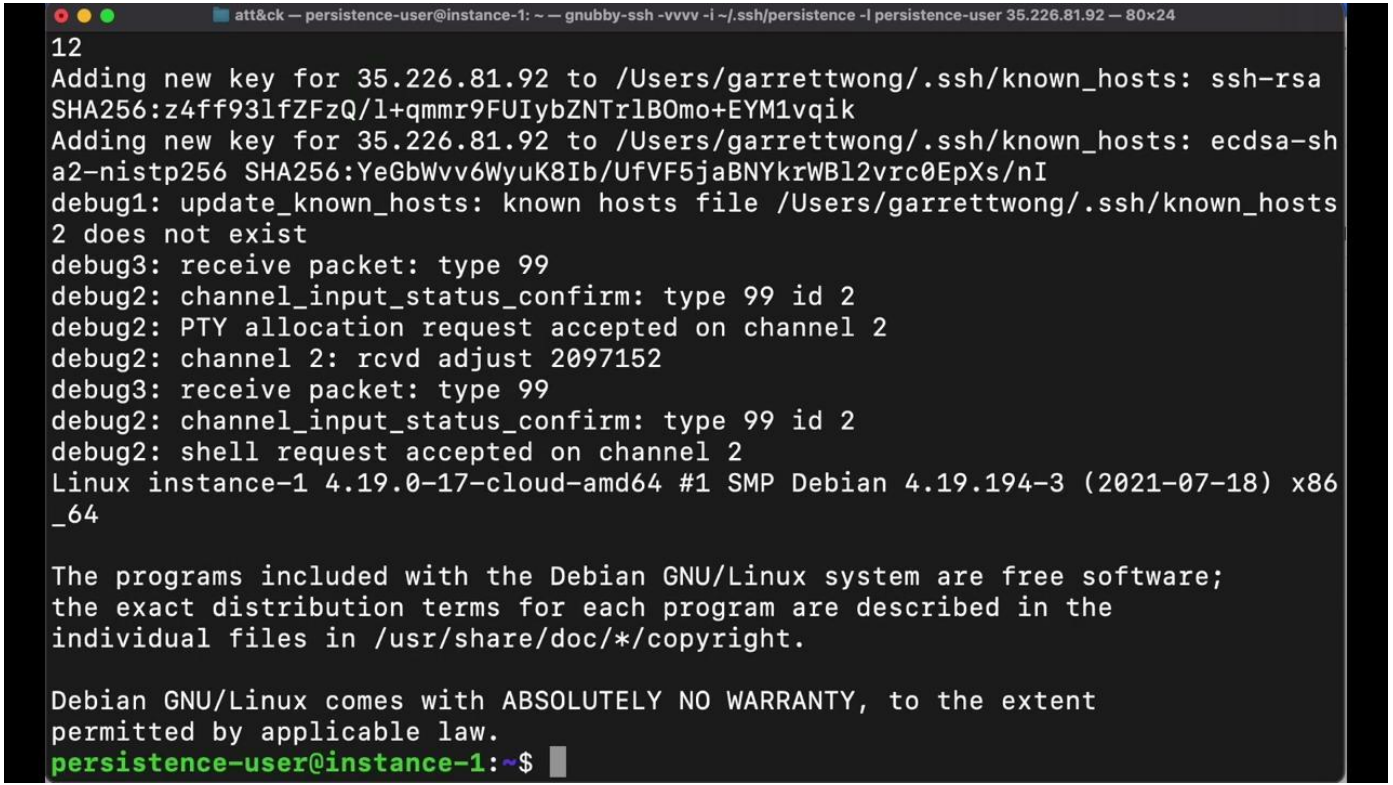
```
cat > metadata-ssh-config << EOF
persistence-user:$SSH_PUB_KEY
EOF

gcloud compute project-info add-metadata \
   --metadata-from-file ssh-keys=metadata-ssh-config

gcloud compute project-info add-metadata \
   --metadata="enable-oslogin=FALSE"
```

Keys to Metadata Server

Persist Login

Persistence: Account Manipulation

Attack



Persistence: Account Manipulation

Detect | Mitigate

Detect Threat

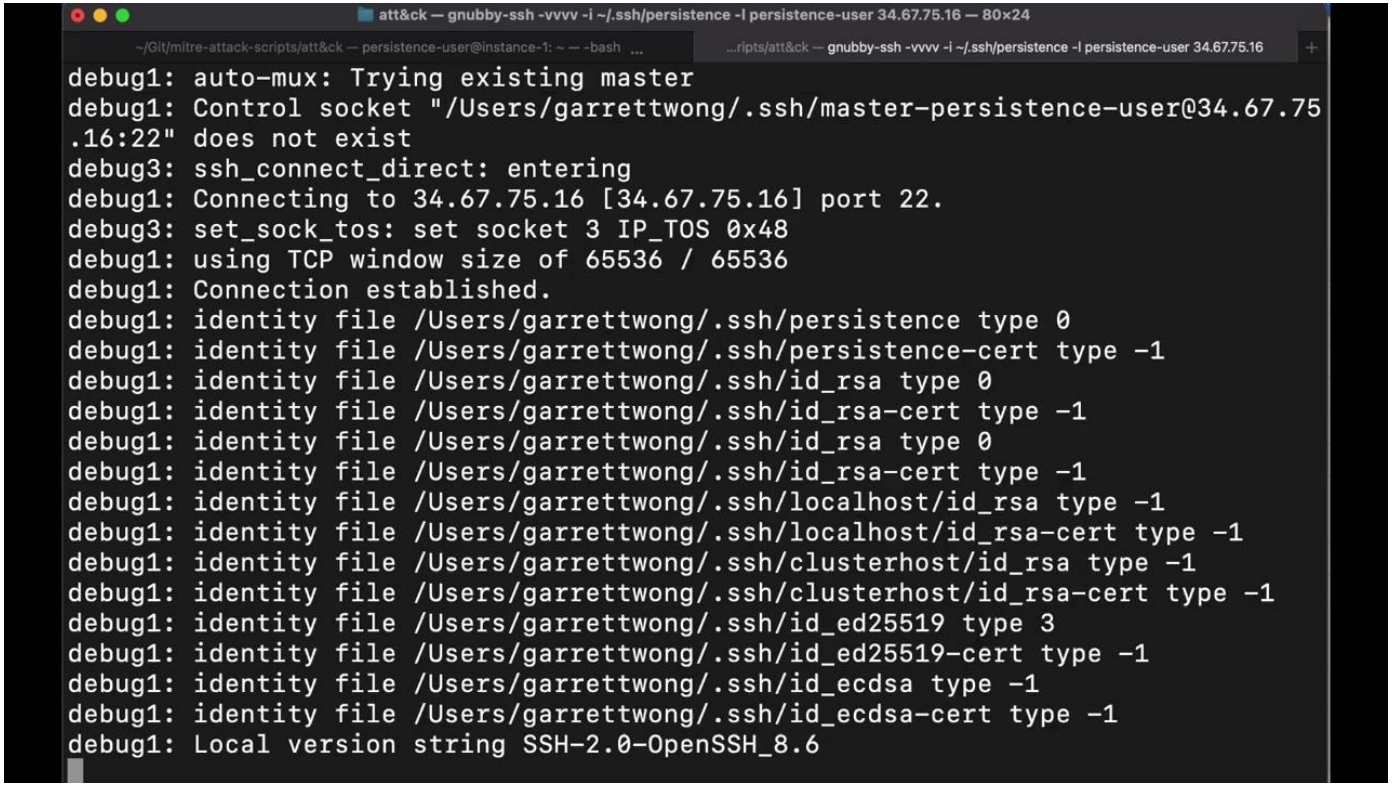
- Detect project and instance metadata changes (Admin Activity logs)
- Detect unrecognized IP addresses (OS Level Logs)

Mitigate Threat

- Enforce OS Login
- Disable Public IPs
- IAP for TCP Forwarding

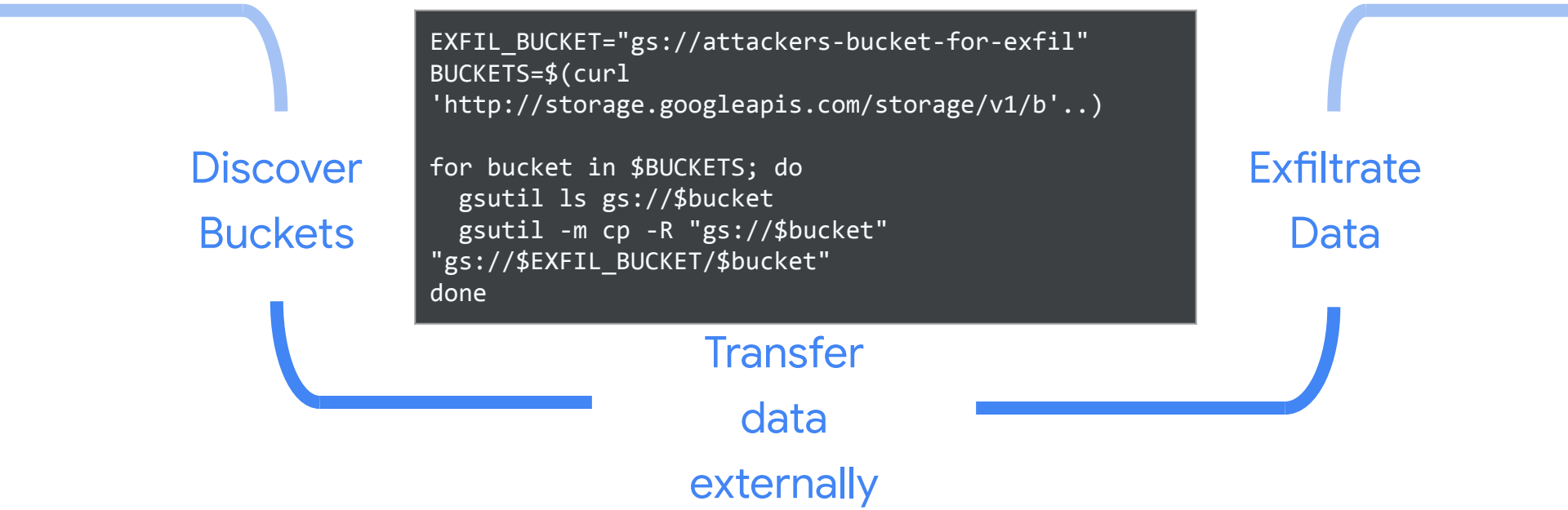
Persistence: Account Manipulation

Mitigating the Attack



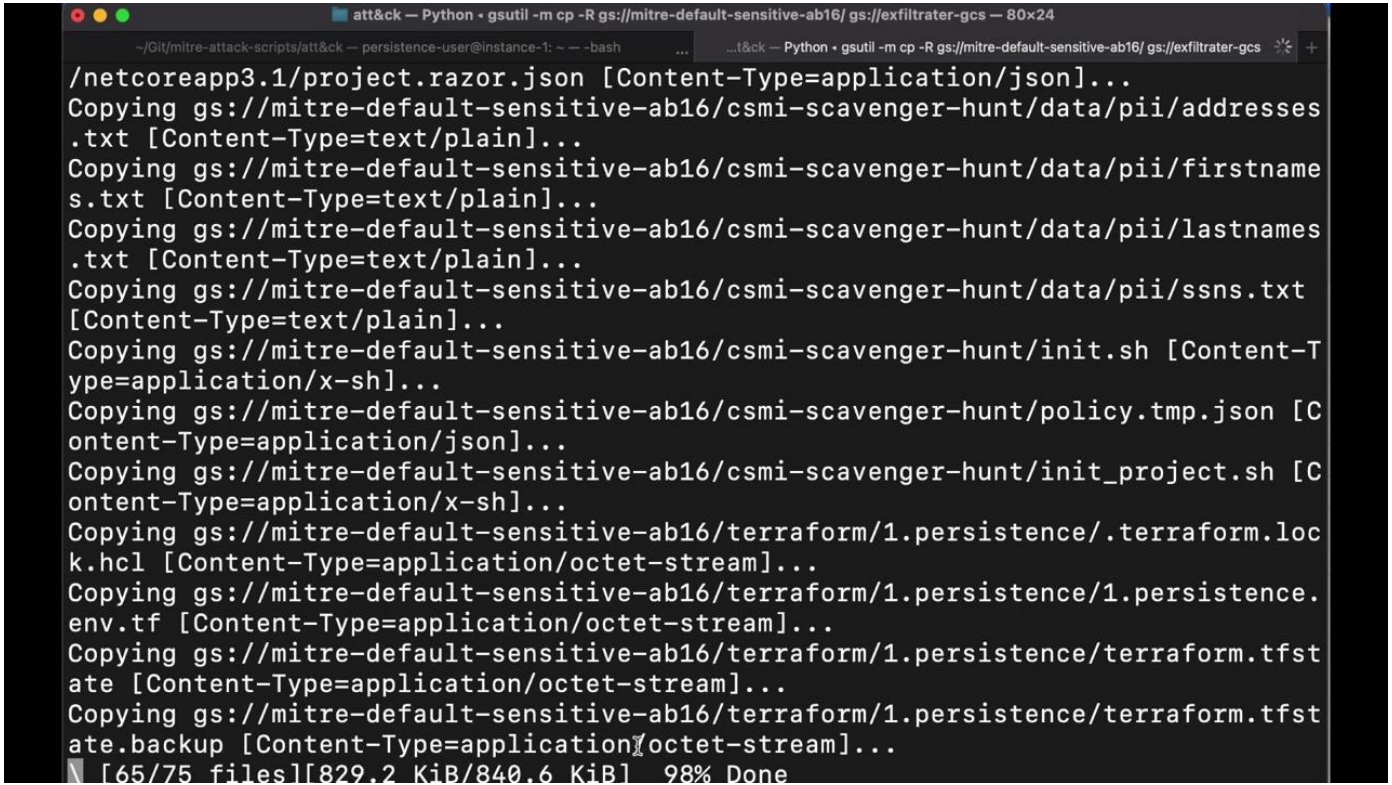
Exfiltration: Transfer Data to Cloud Account

Attack



Exfiltration: Transfer Data to Cloud Account

Attack



Exfiltration: Transfer Data to Cloud Account

Detect | Mitigate

Detect Threat

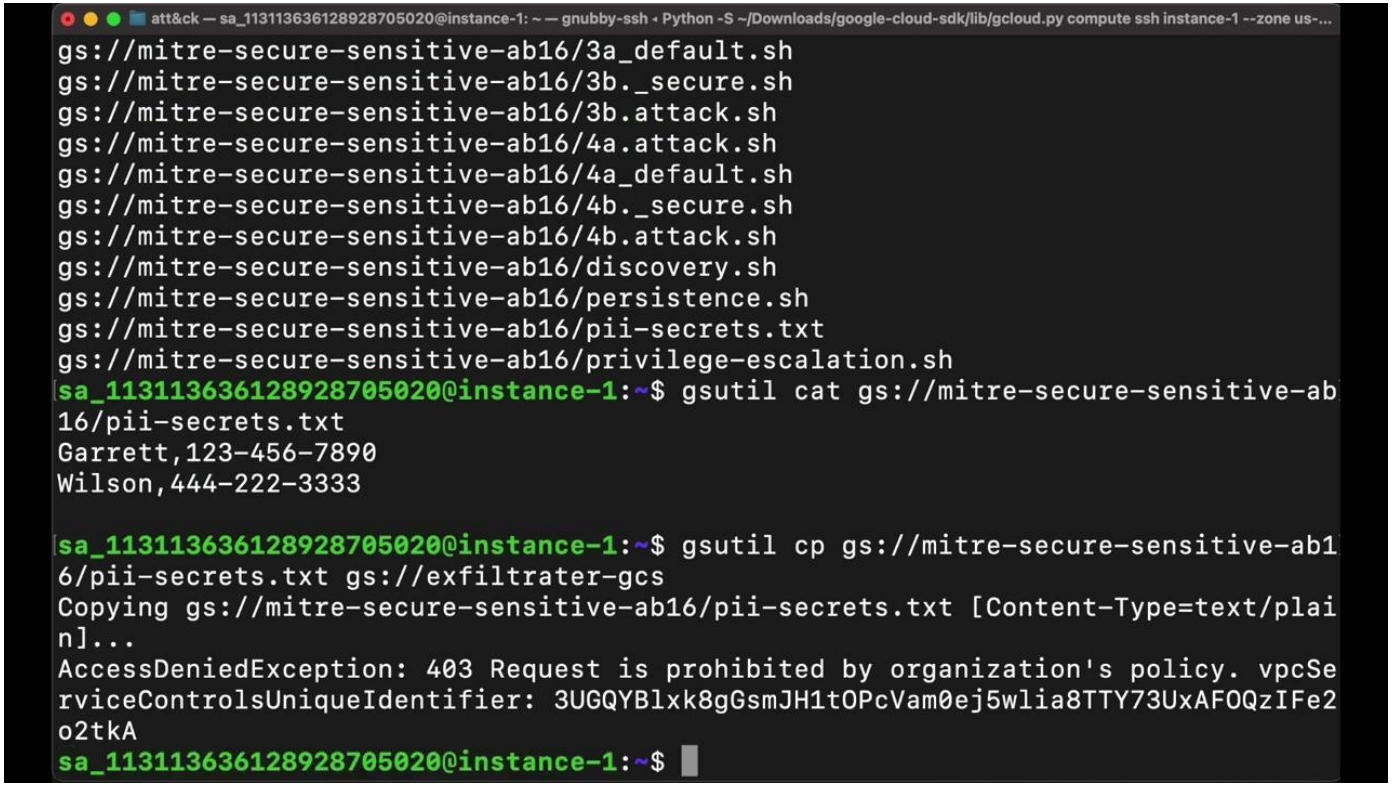
- Data Read to GCS objects (Data Access logs)
- VPC Service Controls Violations (Policy Denied logs)

Mitigate Threat

- VPC Service Controls
- Least Privilege Permission

Exfiltration: Transfer Data to Cloud Account

Mitigating the Attack



Impact: Resource Hijacking

Attack

```
cat > metadata-ssh-config << EOF
persistence-user:$SSH_PUB_KEY
EOF

gcloud compute project-info add-metadata \
   --metadata="enable-oslogin=FALSE"

gcloud compute project-info add-metadata \
   --metadata-from-file ssh-keys=metadata-ssh-config
```

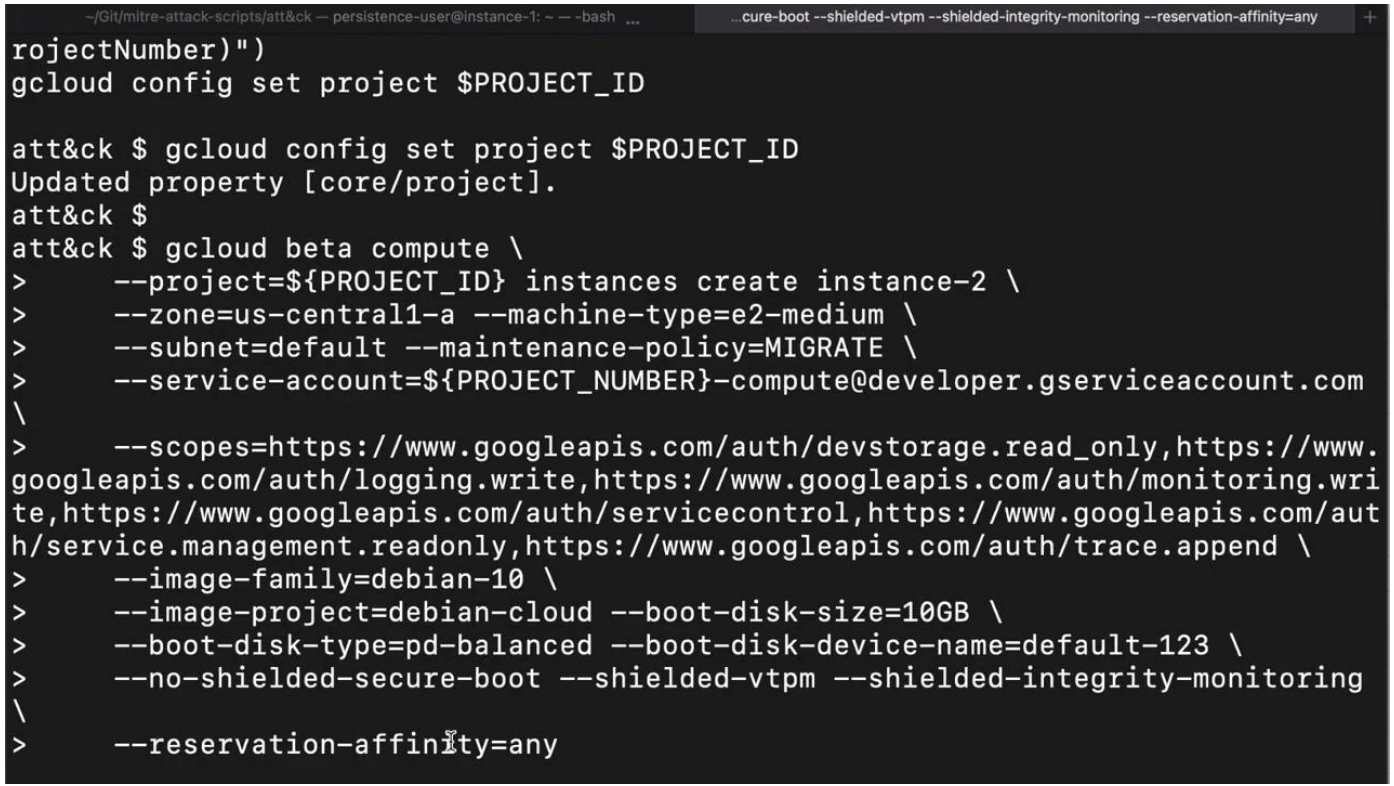
Create VMs

Create NATs

Abuse Resources

Impact: Resource Hijacking

Attack



Impact: Resource Hijacking

Detect | Mitigate

Detect Threat

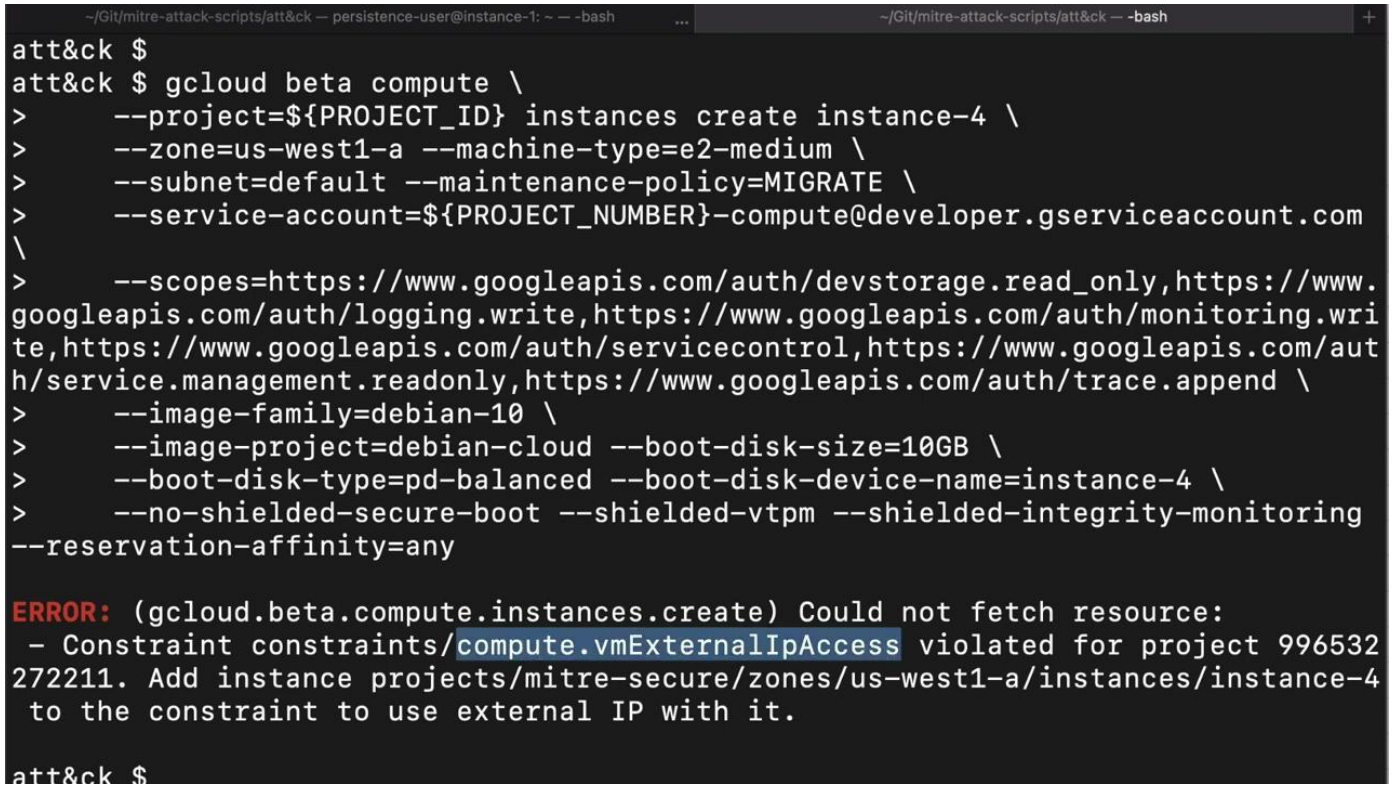
- Anomaly Detection (SCC Findings)
- Cryptomining Detection (SCC Findings)
- Suspicious IPs (Admin Activity logs)
- Org Policy Violation (Admin Activity logs)

Mitigate Threat

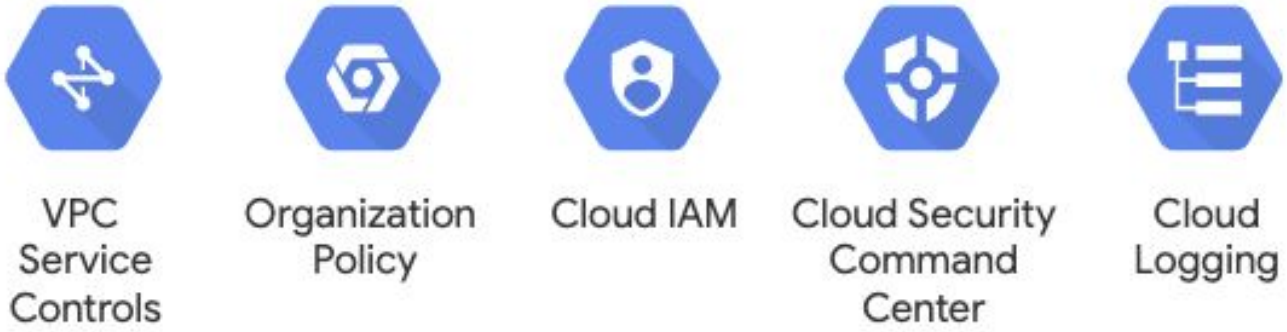
- Organizational Policies
  - Allowed external IPs
  - Restrict Cloud NAT usage
  - Restrict Locations
  - VPC Service Controls

Impact: Resource Hijacking

Mitigating the Attack



Concluding remarks...



GCP Security Foundations White Paper

Sample ATT&CK scripts and logs

Questions?

Feedback Form

https://bit.ly/fwdcs21-wong