Cloud Attacks Update
Motives of Attackers

• Data Theft
• Crypto Mining
• Ransom – Cloud Accounts
• Espionage
• Sabotage
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Examples</th>
<th>Privilege Escalation/Persistence</th>
<th>Impact / End goal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data exfiltration</td>
<td></td>
<td>Data removal/DoS</td>
</tr>
<tr>
<td></td>
<td>Cryptomining</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ransomware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data exfiltration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Initial Access  
Account Discovery
Application Compromise

Examples
Insider Threat
Brute Forcing / Cred Stuffing
Cloud Console / Control Plane

Privilege Escalation/Persistence
Create/Modify accounts/roles
Other cloud accounts

Impact / End goal
Cryptomining
Ransomware
Data exfiltration
Data removal/DoS
Initial Access

- Account Discovery
- Application Compromise

Examples

- Insider Threat
- Brute Forcing / Cred Stuffing
- Cloud Console / Control Plane
- Google Dorks
- Shodan Search
- Vulnerability Exploit

Privilege Escalation/Persistence

- Create/Modify accounts/roles
- Other cloud accounts

Impact / End goal

- Steal Cloud Credentials
- Cryptomining
- Ransomware
- Data exfiltration
- Data removal/DoS
Cloud Console / Control Plane

Insider Threat

Brute Forcing / Cred Stuffing

Cloud Console / Control Plane

Google Dorks

Shodan Search

Vulnerability Exploit

Examples

Privilege Escalation/Persistence

Create/Modify accounts/roles

Other cloud accounts

Spin up instances

Disable services

Deploy containers

VM/Container escape

Impact / End goal

Cryptomining

Ransomware

Data exfiltration

Data removal/DoS

#MiCyberSummit
Initial Access

- Account Discovery
- Application Compromise

Examples

- Insider Threat
- Brute Forcing / Cred Stuffing
- Cloud Console / Control Plane
- Google Dorks
- Shodan Search
- Vulnerability Exploit

Privilege Escalation / Persistence

- Create / Modify accounts / roles
- Other cloud accounts
- Spin up instances
- Disable services
- Deploy containers
- VM / Container escape

Impact / End goal

- Cryptomining
- Ransomware
- Data exfiltration
- Data removal / DoS

# MiCyberSummit
Cloud Console / Control Plane

Insider Threat
Brute Forcing / Cred Stuffing
Cloud Console / Control Plane

Google Dorks
Shodan Search
Vulnerability Exploit

Create/Modify accounts/roles
Other cloud accounts
Spin up instances
Disable services
Deploy containers
VM/Container escape

Cryptomining
Ransomware
Data exfiltration
Data removal/DoS

Initial Access
Examples
Privilege Escalation/Persistence
Impact / End goal

Account Discovery
Application Compromise
Database Discovery

Steal Cloud Credentials

Account Discovery
Application Compromise
Database Discovery

#MiCyberSummit
Cloud Console / Control Plane

Insider Threat
Brute Forcing / Cred Stuffing
Cloud Console / Control Plane

Examples

Google Dorks
Shodan Search
Vulnerability Exploit
Exposed S3 Bucket
Exposed Elasticsearch

Privilege Escalation/Persistence

Create/Modify accounts/roles
Other cloud accounts
Spin up instances
Disable services
Deploy containers
VM/Container escape

Impact / End goal

Cryptomining
Ransomware
Data exfiltration
Data removal/DoS

Account Discovery
Application Compromise
Database Discovery

Initial Access

Steal Cloud Credentials
Cloud Console / Control Plane

Insider Threat
Brute Forcing / Cred Stuffing
Cloud Console / Control Plane

Google Dorks
Shodan Search
Vulnerability Exploit
Exposed S3 Bucket
Exposed Elasticsearch

Create/Modify accounts/roles
Other cloud accounts
Spin up instances
Disable services
Deploy containers
VM/Container escape
Misconfigured services

Cryptomining
Ransomware
Data exfiltration
Data removal/DoS

Initial Access

Examples

Privilege Escalation/Persistence

Impact / End goal

Account Discovery
Application Compromise
Database Discovery

Stolen Cloud Credentials

#MiCyberSummit
Initial Access

- Account Discovery
- Application Compromise
- Database Discovery

Examples

- Insider Threat
- Brute Forcing / Cred Stuffing
- Cloud Console / Control Plane
- Google Dorks
- Shodan Search
- Vulnerability Exploit
- Exposed S3 Bucket
- Exposed Elasticsearch

Steal Cloud Credentials

- Create/Modify accounts/roles
- Other cloud accounts
- Spin up instances
- Disable services
- Deploy containers
- VM/Container escape
- Misconfigured services

Privilege Escalation/Persistence

Impact / End goal

- Cryptomining
- Ransomware
- Data exfiltration
- Data removal/DoS
Initial Access

- Account Discovery
- Application Compromise
- Database Discovery
- API Keys Exposure

Examples

- Insider Threat
- Brute Forcing / Cred Stuffing
- Cloud Console / Control Plane
- Google Dorks
- Shodan Search
- Vulnerability Exploit
- Exposed S3 Bucket
- Exposed Elasticsearch

Privilege Escalation/Persistence

- Create/Modify accounts/roles
- Other cloud accounts
- Spin up instances
- Disable services
- Deploy containers
- VM/Container escape
- Misconfigured services

Impact / End goal

- Cryptomining
- Ransomware
- Data exfiltration
- Data removal/DoS
Cloud Console / Control Plane

Insider Threat
Brute Forcing / Cred Stuffing
Exposed S3 Bucket
Exposed Elasticsearch
Public GitHub Repo
Shodan Search
Google Dorks
Vulnerability Exploit

Initial Access

Account Discovery
Application Compromise
Database Discovery
API Keys Exposure

Examples

Steal Cloud Credentials

Create/Modify accounts/roles
Other cloud accounts
Spin up instances
Disable services
Deploy containers
VM/Container escape
Misconfigured services

Privilege Escalation/Persistence

Impersonation
Social Engineer

Impact / End goal

Data exfiltration
Cryptomining
Ransomware
Data removal/DoS
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Examples</th>
<th>Privilege Escalation/Persistence</th>
<th>Impact / End goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Discovery</td>
<td>Insider Threat</td>
<td>Create/Modify accounts/roles</td>
<td>Cryptomining</td>
</tr>
<tr>
<td></td>
<td>Brute Forcing / Cred Stuffing</td>
<td>Other cloud accounts</td>
<td>Ransomware</td>
</tr>
<tr>
<td></td>
<td>Cloud Console / Control Plane</td>
<td>Spin up instances</td>
<td>Data exfiltration</td>
</tr>
<tr>
<td>Application Compromise</td>
<td>Google Dorks</td>
<td>Disable services</td>
<td>Data removal/DoS</td>
</tr>
<tr>
<td></td>
<td>Shodan Search</td>
<td>Deploy containers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vulnerability Exploit</td>
<td>VM/Container escape</td>
<td></td>
</tr>
<tr>
<td>Database Discovery</td>
<td>Exposed S3 Bucket</td>
<td>Misconfigured services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exposed Elasticsearch</td>
<td>Impersonation</td>
<td></td>
</tr>
<tr>
<td>API Keys Exposure</td>
<td>Public GitHub Repo</td>
<td>Social Engineer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compromised Dev Machine</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Account Discovery**
- **Application Compromise**
- **Database Discovery**
- **API Keys Exposure**
Initial Access

- Account Discovery
- Application Compromise
- Database Discovery
- API Keys Exposure

Examples

- Insider Threat
- Brute Forcing / Cred Stuffing
- Cloud Console / Control Plane
- Google Dorks
- Shodan Search
- Vulnerability Exploit
- Exposed S3 Bucket
- Exposed Elasticsearch
- Public GitHub Repo
- Compromised Dev Machine

Privilege Escalation/Persistence

- Create/Modify accounts/roles
- Other cloud accounts
- Spin up instances
- Disable services
- Deploy containers
- VM/Container escape
- Misconfigured services
- Impersonation
- Social Engineer

Impact / End goal

- Cryptomining
- Ransomware
- Data exfiltration
- Data removal/DoS