Manipulate Cloud Configuration (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Both Azure and AWS have numerous configuration options for security controls and logging that can be altered through their portals or through command line tools. Some of these configurations are subtle and might not be noticed even if people ae actively monitoring API logs such as AWS CloudTrail. An adversary can take advantage of these configurations such as reducing the detail of logging actions. Because most automated analytics depend on raw cloud events, reducing the frequency and detail of these events will necessarily impact the ability of analytics to recognize malicious behavior.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Detection\_disruption | Publicly available Pacu module that allows an adversary to make one or more subtle changes to AWS logging without invoking more noticeable actions like deletion or disabling. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Audit | | Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources. Consider using automated resource checkers such as CloudSploit or Divvycloud. |
|  | AWS | To perform an audit via AWS it is suggested to review information such as account details (credentials, users, groups, roles, etc), mobile applications, EC2 configurations, policies, and account activity. How to audit these different factors can be found in detail at: **https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html.** |
|  | Azure | To perform an audit via Azure an administrator can review the audit logs that are recorded under Azure’s monitoring for active directory. The audit logs allow for filtering, as well as looking at users, groups, and enterprise specific information. Full details on how to access this information can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.** |
|  | GCP | To perform an audit via GCP the logs can be reviewed. GCP breaks this down into three categories; admin activity, data access, and system events. The audit logs can be viewed a few different ways- the console, API, or gcloud. Full details on how to view these logs, how to export, and for how to configure the retention period can be found here: **https://cloud.google.com/logging/docs/audit.** |

Detection

 CloudTrail or Monitor will record accesses to the cloud API when changes are made to logging services.

References

1. https://github.com/RhinoSecurityLabs/pacu/wiki/Module-Details - Accessed Feb 12, 2020