Cloud Log Scrubbing (version 1.0)

**Cloud Service Label: IaaS, PaaS, SaaS**

Description

Deletion of logs has been a universal technique of adversaries since the dawn of intrusions. Cloud platforms make this practice far more convenient and thorough because most cloud services have a unified interface for accessing and collecting logs from disparate cloud services. With legacy networks it would have required effort for an adversary to determine how a victim was logging each service and where the logs might reside. Logging is now a largely standardized process thanks to Azure and AWS efforts. Adversaries can use cloud provided API’s and logic functions to quickly eliminate problematic log entries. Cloud logs usually leverage standard Cloud object storage which subjects them to data attacks associated with any data stored in Cloud object storage.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Weird All Cloud Trail Cleaning Scripts | Publicly available scripts to remove log entries from AWS Cloud Trail. |
| Pacu | Pacu’s plug-in modules offer assistance for enumeration, privilege escalation, data exfiltration, service exploitation, and log manipulation within AWS. |
| Delete all AWS logs | The *delete\_all\_awslogs.sh* script will delete AWS logs for a specified region. You can also specify log group names like */aws/lambda*. |
| Delete Azure Analytics Logs workspace | Adding a ‘-ForceDelete’ tag to the Azure CLI deletion command will permanently delete a workspace. |

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.** |
| Permissions | | Remove delete permissions to logs associated storage objects from most accounts. |
| Offsite Storage/Processing | | Quickly move logs off the cloud to a local repository,SIEM, or to another separate account owner within the cloud. |
| Recover Azure Log Analytics Workspace | | If an Azure Log Analytics workspace is deleted, the workspace is placed in a soft-delete state, which can be used to recover the deleted data, configuration, and connected agents. |

Detection

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for CloudTrail | To create a metric filter and alarm:   1. Create a filter that checks for CloudTrail changes and the specific *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic that the alarm will notify 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter from step 1 and SNS topic in step 2 |
| Create Activity Log Alerts in Azure | To create log activity alerts for deletion in the Azure Console:   1. Navigate to *Monitor’ / ‘Alerts* 2. Select *Manage alert rules* 3. Click on the Alert *Name* where Condition contains *operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete* 4. Hover a mouse over *Condition* to ensure it is set to *Whenever the Administrative Activity Log “Delete Security Rule (networkSecurityGroups/securityRules)” has “any” level with “any” status and event is initiated by “any*” |

References

1. [https://github.com/carnal0wnage/weirdAAL/wiki/Usage](https://b0k103-cportal2.mitre.org/carnal0wnage/weirdAAL/wiki/,DanaInfo=.agjvkygFjwv,SSL+Usage) - Accessed Feb 22,2020
2. <https://github.com/RhinoSecurityLabs/pacu>. Accessed August 5, 2020.
3. <https://gist.github.com/pahud/1e875cb1252a622173cc2236be5c2963>. Accessed August 5, 2020.
4. <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-delete-trails-console.html>. Accessed August 5, 2020.
5. <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/delete-workspace>. Accessed August 5, 2020.