Accessing Data from Databases (version 1.0)

**Cloud Service Label: PaaS**

Description

Both AWS and Azure have PaaS offerings for database services that are very popular. Such services can still allow traditional database access using SQL commands from the host running the SQL instance but more interestingly, a REST-based API which enables a richer, less restricted method of controlling the database. Adversaries with some cloud credentials may be able to use this API to access data from the database that more traditional SQL access might prohibit.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Snapshot-rds | Public Nimbostratus module that abuses ability to request a snapshot of a database. Adversary then restores DB snapshot on a host that the adversary controls. This gives adversary complete access to all table data. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Carefully assign permissions to database API | | Care must be taken to enable read access to a database without permitting additional functionality such as create snapshots. |
|  | AWS | API developers will require escalated permissions to the API gateway. Information on how to properly configure API permissions on AWS can be found here: https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html. |
|  | Azure | There is an API permissions page within the Azure portal that can give developers the escalated permissions they need to perform their tasks, but should be monitored and only given to those who need such permissions. Microsoft documentation outlines how to give specific permissions, as well as how resource applications can expose scopes and application roles to client applications. Both can be useful when assigning correct permissions. Documentation can be found here: https://docs.microsoft.com/en-us/azure/active-directory/develop/perms-for-given-api#recommended-documents. |

Detection

In theory requests made of the API for DB table snapshots should be captured in cloud API logs such as Azure Monitor logs and CloudTrail.

References

1. <http://andresriancho.github.io/nimbostratus/>. Accessed Feb 23, 2020