Cloud Instance Metadata API (version 1.0)

**Cloud Service Label: IaaS**

Description

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data. Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and User Data scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, attackers may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows the attacker to gain access to the sensitive information via a request to the Instance Metadata API.

The de facto standard across cloud service providers is to host the Instance Metadata API at  http://169.254.169.254.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Capital One Breach | Capital One Breach where a SSRF on a vulnerable application hosted on an AWS server allowed adversary to access server’s metadata instance and forward WAF account credentials back to a local workstation. These credentials had read permissions to numerous S3 buckets for the organization. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Name** | | **Description** |
| [Filter Network Traffic](https://attack.mitre.org/mitigations/M1037) | | Cloud service providers support IP-based restrictions when accessing cloud resources. Consider using IP whitelisting along with user account management to ensure that data access is restricted not only to valid users, but only from expected IP ranges to mitigate the use of stolen credentials to access data. |
|  | AWS | An AWS environment can be configured with network ACLs (access control lists) to allow or deny inbound and outbound traffic. This can be accomplished by accessing Amazon VPC and navigating to either inbound or outbound rules depending on the rule the user wishes to add and they can be added, removed, or edited from that panel. Full details about ACLs and how to add rules in AWS can be found here: **https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html.** |
|  | Azure | In Azure storage resources can be tied exclusively to a particular virtual network reducing the chances that it can be accessed externally or from other cloud assets. This can be done multiple ways including the Azure Portal, Azure PowerShell, and Azure CLI (Command Line Interface). Depending on the method used to implement this the procedure can vary, but will include the need to create a security group, create a network security group, associate that network security group with a specific subnet and then create security rules that are associated to the inbound and outbound rules for that subnet. Full details on how to configure this utilizing the various methods can be found below:  Azure Portal: **https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic**  Azure PowerShell: **https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic-powershell**  Azure CLI: **https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic-cli** |
| Use AWS update | | AWS metadata service v2 could mitigate Capitol One example, though it is not foolproof and not all encompassing. There are tools that can help with transitioning to V2 such as CloudWatch. For detailed information on the differences between V1 and V2, as well as how to transition from V1 to V2, please refer to AWS documentation at: [**https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html)**.** |

Detection

Monitor access to the Instance Metadata API and look for anomalous queries. It may be possible to detect adversary use of credentials they have obtained. See [Valid Accounts](https://attack.mitre.org/techniques/T1078) for more information.

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |
| 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*” |
| Create, View, and Manage Activity Alerts in Azure Monitor | To create a log alert in the Azure portal:   1. Select **Monitor -> Alerts** 2. Select **New alert rule** of the **Alerts** window 3. Provide information in **Define alert condition** 4. Provide details in **Define alert details** 5. Specify action group for new alert rule under **Action group**, or create a new action group with + **New group** 6. Select **Yes** for the **Enable rule upon creation** option 7. Select **Create alert rule**   To view and manage alerts:   1. Select **Monitor -> Alerts -> Manage alert rules** 2. Select the rule you want to modify and double-click to edit the rule options 3. Click **Save** |
| Azure Resource Manager Templates | Azure Resource Manager templates in the format of JSON files that can be used to configure metric alerts in Azure Monitor. These templates can be used for simple static and dynamic threshold metric alerts, availability tests, and monitoring multiple resources. |
| Enable CloudTrail across all regions in AWS | To enable CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |

References

1. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html. Retrieved February 3, 2020
2. https://redlock.io/blog/instance-metadata-api-a-modern-day-trojan-horse. Retrieved July 16, 2019
3. https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/. Retrieved June 8, 2020