Data Collected from Cloud Storage Object (combined with S3/Blob manipulation) (version 1.0)

**Cloud Service Label: IaaS**

Description

Adversaries may access data objects from improperly secured cloud storage.

Many cloud service providers offer solutions for online data storage such as Amazon S3, Azure Storage, and Google Cloud Storage. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider's APIs. Solution providers typically offer security guides to help end users configure systems.

Misconfiguration by end users is a common problem. There have been numerous incidents where cloud storage has been improperly secured (typically by unintentionally allowing public access by unauthenticated users or overly-broad access by all users), allowing open access to credit cards, personally identifiable information, medical records, and other sensitive information. Adversaries may also obtain leaked credentials in source repositories, logs, or other means as a way to gain access to cloud storage objects that have access permission controls.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| S3\_download\_Bucket | Publicly available Pacu module that scans the current account for AWS buckets and prints/stores as much data as it can about each one. With no arguments, this module will enumerate all buckets the account has access to, then prompt you to download all files in the bucket or not. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| [Audit](https://attack.mitre.org/mitigations/M1047) | | 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.** |
| [Encrypt Sensitive Information](https://attack.mitre.org/mitigations/M1041) | | Encrypt data stored at rest in cloud storage. Managed encryption keys can be rotated by most providers. At a minimum, ensure an incident response plan to storage breach includes rotating the keys and test for impact on client applications. |
|  | AWS | To encrypt data at rest in an AWS environment first start by configuring the IAM roles and permissions. A policy will need to be created to specify that the data is to be encrypted and then the policy is attached to the instance. Full details on how to accomplish this can be found at: **https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption/**. |
|  | Azure | To encrypt data at rest in an Azure environment it can be done differently depending on the cloud service the customer is utilizing. For SaaS customers this can be enabled or available on each specific service. For PaaS customers there are specific storage and application platforms that can be used. In terms of IaaS customers this can be broken down to a couple different aspects. Encrypted storage can be enabled the same as PaaS services, utilizing other Azure services. Encrypted compute allows for all managed disks, snapshots, and images to be encrypted utilizing a service managed key. The keys are stored in the Azure key vault. Full details on how to accomplish this can be found at: [**https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest**](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest)**.** |
| [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** |
| [Multi-factor Authentication](https://attack.mitre.org/mitigations/M1032) | | Use multi-factor authentication for user and privileged accounts. Do not manage Cloud portals from machines that perform user email and web browsing tasks. All users should be required to utilize two factor authentication. |
|  | *AWS* | This can be enforced by first creating a policy that would prohibit actions except those that allow a user to change their password or manage 2FA, then attaching a policy to a group that includes all user accounts where they can be allowed all access if they sign in with 2FA. Once these actions are completed it should be tested to verify the access is given correctly. To see full details on how to complete this view AWS documentation at: **https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\_users-self-manage-mfa-and-creds.html.** |
|  | *Azure* | This can be done by creating a MFA registration policy. It can than be assigned to all users (with the ability to exclude some if need be, but is not recommended). Make sure once the policy is created and added to users that it is then being enforced, once enforced it should be tested for verification. To see full details on how to complete this view Azure documentation at: **https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy.** |
|  | *GCP* | This can be done by first enabling it on the current account being used by admin to assign the roles, then enable two factor on an instance by instance or project by project basis, then assigning the requirements based on IAM roles and applying it to all users. To see full details on how to complete this view Azure documentation at: **https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication.** |
| [Restrict File and Directory Permissions](https://attack.mitre.org/mitigations/M1022) | | Users should have limited access to files and directories depending on their need for access. The file and directory permissions should be restricted on the basis of least privilege. |
|  | AWS | To manage the files and directory permissions in AWS, IAM policies can be used. This can be done by utilizing group policies and policy variables. The policy would be created specifying the folder, then the permissions attached to that folder (whether the user has access to list out the objects within the directory, if they have read permissions, if they have write permissions, etc.), lastly the group that it applies to would be specified. The users can that be added and removed from that group as needed. Full details on how this can be done is explained here: **https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/.** |
|  | Azure | To manage the files and directory permissions in an Azure environment basic and advanced system defined controls. This will be dependent on the type of system being used (Windows, Linux, etc). The permissions will be set individually or by group using the system commands or controls needed.. Full details on how this can be done is explained here:[**https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-configure-permissions**](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-configure-permissions)**.** |

Detection

Monitor for unusual queries to the cloud provider's storage service. Activity originating from unexpected sources may indicate improper permissions are set that is allowing access to data. Additionally, detecting failed attempts by a user for a certain object, followed by access to the same object may be an indication of suspicious activity.

References

1. [Amazon. (2019, May 17). How can I secure the files in my Amazon S3 bucket?. Retrieved October 4, 2019.](https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/)

1. [Amlekar, M., Brooks, C., Claman, L., et. al.. (2019, March 20). Azure Storage security guide. Retrieved October 4, 2019.](https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide" \t "_blank)

1. [Google. (2019, September 16). Best practices for Cloud Storage. Retrieved October 4, 2019.](https://cloud.google.com/storage/docs/best-practices" \t "_blank)

1. [Trend Micro. (2017, November 6). A Misconfigured Amazon S3 Exposed Almost 50 Thousand PII in Australia. Retrieved October 4, 2019.](https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/a-misconfigured-amazon-s3-exposed-almost-50-thousand-pii-in-australia" \t "_blank)

1. [Barrett, B.. (2019, July 11). Hack Brief: A Card-Skimming Hacker Group Hit 17K Domains—and Counting. Retrieved October 4, 2019.](https://www.wired.com/story/magecart-amazon-cloud-hacks/" \t "_blank)

1. [HIPAA Journal. (2017, October 11). 47GB of Medical Records and Test Results Found in Unsecured Amazon S3 Bucket. Retrieved October 4, 2019.](https://www.hipaajournal.com/47gb-medical-records-unsecured-amazon-s3-bucket/" \t "_blank)

1. [Amazon. (n.d.). Temporary Security Credentials. Retrieved October 18, 2019.](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html" \t "_blank)

1. [Google. (n.d.). Key rotation. Retrieved October 18, 2019.](https://cloud.google.com/kms/docs/key-rotation" \t "_blank)