Account Manipulation (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Account manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment. Manipulation could consist of modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to subvert password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.

*Azure AD*

In Azure, an adversary can set a password for Service Principals, which is an application specific method of accessing Azure resources. This could facilitate persistence to all Azure services the SP has access to without using an actual user’s credentials. Azure also allows alternative authentication mechanisms such as SAS tokens and certificates to be created and used rather than passwords for Azure services.

*AWS*

AWS policies allow trust between user accounts in different AWS accounts by simply identifying an external Amazon account ID and assigning it to a native role within the existing AWS account. It is then up to the cloud admin to notice that this has happened and that the role assigned to the trusted account is permissible.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Skeleton Key | This exploit is possible after an adversary compromises a server that is running an Azure agent. Once compromised the authentication flow that is used to verify credentials can be tampered with. This attack requires privileged access to complete. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| [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. |
|  | *AWS* | All users should be required to utilize two factor authentication. 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* | All users should be required to utilize two factor authentication. 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* | All users should be required to utilize two factor authentication. 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.** |
| [Account Segmentation](https://attack.mitre.org/mitigations/M1030) | | Consider separating different resources under different administrative domains so that credential compromise does not put all assets in danger. In the case of Azure, multiple subscriptions can be created with different administrators that can only access resources within the subscription. The subscriptions can still belong under the same Azure account for overall accounting and administration/policy. |
| [AD Server Configuration](https://attack.mitre.org/mitigations/M1028) | | Use Cloud provided AD services rather than maintaining AD servers in the cloud. |
| [Privileged Account Management](https://attack.mitre.org/mitigations/M1026) | | Do not allow subscription-level administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems. This can be done by first limiting the access that these accounts have outside of the administrative rights, but then also monitoring (details in detection) for events that might show a compromised account. |
|  | AWS | To manage the access that privileged accounts have on the AWS cloud system to only allow administrators to perform administrative tasks on such accounts can be accomplished utilizing limited IAM administrator accounts. To configure this the administrator would have two accounts; one would have administrative rights and no basic access while the other account has basic access with no administrative rights. To limit the administrative account the IAM limited administrator would be used. This is done by creating a policy that gives a user admin rights, but disallows the other actions using the AWS command line interface. This is outlined at: [**https://aws.amazon.com/blogs/security/how-to-create-a-limited-iam-administrator-by-using-managed-policies/**](https://aws.amazon.com/blogs/security/how-to-create-a-limited-iam-administrator-by-using-managed-policies/)**.** |
|  | Azure | To manage the access that privilege accounts have on the Azure cloud system to only allow administrators to perform administrative tasks on such accounts can be accomplished utilizing limited IAM administrator accounts. To configure this the administrator would have two accounts; one would have administrative rights and no basic access while the other account has basic access with no administrative rights. To limit the administrative account the specific administrative needs can be picked from a number of options available (Azure DevOps Administrator, Billing Administrator, Cloud Application Administrator, etc.) These different options can be edited to fit the needs and limit the basic access. This is outlined at: [**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles**](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles)**.** |
|  | GCP | To manage the access that privilege accounts have on the Azure cloud system to only allow administrators to perform administrative tasks on such accounts can be accomplished utilizing limited IAM administrator accounts. To configure this the administrator would have two accounts; one would have administrative rights and no basic access while the other account has basic access with no administrative rights. To limit the administrative account pre-defined administrator accounts can be used (mobile admin, Google voice admin, help desk admin, etc.). These accounts can be used with their pre-defined settings, or modified depending on specific use cases. These can limit access to basic functionality needed. This is outlined at: [**https://support.google.com/a/answer/2405986?hl=en**](https://support.google.com/a/answer/2405986?hl=en)**.** |

Detection

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Monitoring | | Collect events that correlate with changes to account objects on systems and the domain. Monitor for modification of accounts in correlation with other suspicious activity. Changes may occur at unusual times or from unusual systems. Especially flag events where the subject and target accounts differ or that include additional flags such as changing a password without knowledge of the old password. Use of credentials may also occur at unusual times or to unusual systems or services and may correlate with other suspicious activity |
|  | AWS | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3.  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 |
|  | 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.  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** |

References

1. https://www.scmagazineuk.com/hackers-manipulate-azure-agent-using-skeleton-key-attack-cloud-infrastructure/article/1681074. Accessed June 15, 2020