Utilize Breach Replay (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Credentials for accessing Azure and AWS portals/API are often reused for other web-based accounts by both privileged Azure and AWS users. These other accounts may be compromised, and adversaries will as a matter of course attempt to use harvested credentials to access Cloud-based resources knowing the prevalence of password reuse.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Harvesting of Common Passwords from Multiple Accounts | Microsoft recently has conducted an extensive study of credentials they have detected throughout all their platforms and found 44 million credentials shared between Azure and other unrelated accounts. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Good Password Practices | | Ensure good password practices. Never use Azure and AWS passwords for any other cloud or computer access. |
|  | AWS | Good password practices can be enforced in AWS via the console, AWS CLI, and AWS API. These configurations are for IAM accounts only and have a range of different characteristics that can be enforced. For instance minimum password length, require a range of characters (lowercase, uppercase, number, and non alphanumeric ), allow users to change their own password, password expiration, prevent password reuse, and require administrator reset after password expiration. All details on how to configure these enforcement policies with all three management systems can be found here: **https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_passwords\_account-policy.html.** |
|  | Azure | Good password practices can be enforced in Azure only with managed domains created using the resource manager deployment. By default these accounts have some policies enforced including amount of lockout duration, allowed number of logon attempts, Reset failed logon attempts count after 30 minutes, and lifetime of password. Other policies that can be changed are minimum password length and the ability to enforce the concept of ‘passwords must meet complexity requirements’. These configurations can be accomplished by accessing the Active Directory Administrative Center under administrative tools, then editing the rules under the settings for the Password Settings Container. Full details on how to accomplish this can be found here: **https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy.** |
| Multi-Factor Authentication | | 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.** |

Detection

In Azure all user logins are recorded under the Azure Active Directory Sign-ins blade. This information can also be downloaded to a central SIEM for correlation. Assess logins and their originating location against expected behavior. If in Azure a user has the P2 Active Directory licensing, Azure Identity protection may alert you to the presence of this attack based on Microsoft’s experience with other Microsoft customers.

References

1. https://www.microsoft.com/securityinsights/Identity. Accessed Feb 20, 2020
2. https://docs.microsoft.com/en-gb/azure/active-directory/identity-protection/overview-identity-protection. Accessed Feb 20, 2020