Permission Groups Discovery (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Adversaries may attempt to find local system or domain-level groups and permissions settings.

*Office 365 and Azure AD*

With authenticated access there are several tools that can be used to find permissions groups. The Get-MsolRole PowerShell cmdlet can be used to obtain roles and permissions groups for Exchange and Office 365 accounts.

Azure CLI (AZ CLI) also provides an interface to obtain permissions groups with authenticated access to a domain. The command az ad user get-member-groups will list groups associated to a user account.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Manage log data like other sensitive data | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |

Detection

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with API to gather information. Monitor the API logs in Azure and AWS for queries regarding Permission Groups.

References