Network Share Discovery (version 1.0)

**Cloud Service Label: IaaS**

Description

Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.

Cloud virtual networks may contain remote network shares or file storage services accessible to an adversary after they have obtained access to a system. For example, AWS and Azure support creation of Network File System (NFS) shares and Server Message Block (SMB) shares that may be mapped on endpoint or cloud-based systems.

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

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

In cloud-based systems, native logging can be used to identify access to certain APIs and dashboards that may contain system information. Depending on how the environment is used, that data alone may not be sufficient due to frequent use during normal operations.

References