System Network Connections Discovery (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network or by sniffing network traffic that the machine can see.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers have different ways in which their virtual networks operate, but the basic concepts are the same.

Examples

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

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
|  | 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 the Windows API to gather information. Information may also be acquired through  PowerShell or the CLI.

References