Remote Services: Direct Cloud VM Connections, Sub-technique T1021.008 - Enterprise

Archived: 2026-04-05 13:34:57 UTC

Adversaries may leverage Valid Accounts to log directly into accessible cloud hosted compute infrastructure through cloud native methods. Many cloud providers offer interactive connections to virtual infrastructure that can be accessed through the Cloud API, such as Azure Serial Console[1], AWS EC2 Instance Connect[2][3], and AWS System Manager.[4].

Methods of authentication for these connections can include passwords, application access tokens, or SSH keys. These cloud native methods may, by default, allow for privileged access on the host with SYSTEM or root level access.

Adversaries may utilize these cloud native methods to directly access virtual infrastructure and pivot through an environment.[5] These connections typically provide direct console access to the VM rather than the execution of scripts (i.e., Cloud Administration Command).

Source: https://attack.mitre.org/techniques/T1021/008