Wi-Fi Networks, Technique T1669 - Enterprise

Archived: 2026-04-05 15:04:12 UTC

Adversaries may gain initial access to target systems by connecting to wireless networks. They may accomplish this by exploiting open Wi-Fi networks used by target devices or by accessing secured Wi-Fi networks — requiring Valid Accounts — belonging to a target organization.[1][2] Establishing a connection to a Wi-Fi access point requires a certain level of proximity to both discover and maintain a stable network connection.

Adversaries may establish a wireless connection through various methods, such as by physically positioning themselves near a Wi-Fi network to conduct close access operations. To bypass the need for physical proximity, adversaries may attempt to remotely compromise nearby third-party systems that have both wired and wireless network connections available (i.e., dual-homed systems). These third-party compromised devices can then serve as a bridge to connect to a target's Wi-Fi network.[2]

Once an initial wireless connection is achieved, adversaries may leverage this access for follow-on activities in the victim network or further targeting of specific devices on the network. Adversaries may perform Network Sniffing or Adversary-in-the-Middle activities for Credential Access or Discovery.

Source: https://attack.mitre.org/techniques/T1669