# TTP Detail – T1669

## TTP Information

Name: Wi-Fi Networks

Description: 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](https://attack.mitre.org/techniques/T1078) — belonging to a target organization.(Citation: DOJ GRU Charges 2018)(Citation: Nearest Neighbor Volexity) 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.(Citation: Nearest Neighbor Volexity)

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](https://attack.mitre.org/techniques/T1040) or [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) activities for [Credential Access](https://attack.mitre.org/tactics/TA0006) or [Discovery](https://attack.mitre.org/tactics/TA0007).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: initial-access

## APTs (Intrusion Sets)

* APT28