# TTP Detail – T1557.004

## TTP Information

Name: Evil Twin

Description: Adversaries may host seemingly genuine Wi-Fi access points to deceive users into connecting to malicious networks as a way of supporting follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or [Input Capture](https://attack.mitre.org/techniques/T1056).(Citation: Australia ‘Evil Twin’)  
  
By using a Service Set Identifier (SSID) of a legitimate Wi-Fi network, fraudulent Wi-Fi access points may trick devices or users into connecting to malicious Wi-Fi networks.(Citation: Kaspersky evil twin)(Citation: medium evil twin) Adversaries may provide a stronger signal strength or block access to Wi-Fi access points to coerce or entice victim devices into connecting to malicious networks.(Citation: specter ops evil twin) A Wi-Fi Pineapple – a network security auditing and penetration testing tool – may be deployed in Evil Twin attacks for ease of use and broader range. Custom certificates may be used in an attempt to intercept HTTPS traffic.   
  
Similarly, adversaries may also listen for client devices sending probe requests for known or previously connected networks (Preferred Network Lists or PNLs). When a malicious access point receives a probe request, adversaries can respond with the same SSID to imitate the trusted, known network.(Citation: specter ops evil twin) Victim devices are led to believe the responding access point is from their PNL and initiate a connection to the fraudulent network.  
  
Upon logging into the malicious Wi-Fi access point, a user may be directed to a fake login page or captive portal webpage to capture the victim’s credentials. Once a user is logged into the fraudulent Wi-Fi network, the adversary may able to monitor network activity, manipulate data, or steal additional credentials. Locations with high concentrations of public Wi-Fi access, such as airports, coffee shops, or libraries, may be targets for adversaries to set up illegitimate Wi-Fi access points.

## Threat-Mapped Scoring

Score: 3.9

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: collection

## APTs (Intrusion Sets)

* APT28