# TTP Detail – T1016.002

## TTP Information

Name: Wi-Fi Discovery

Description: Adversaries may search for information about Wi-Fi networks, such as network names and passwords, on compromised systems. Adversaries may use Wi-Fi information as part of [Account Discovery](https://attack.mitre.org/techniques/T1087), [Remote System Discovery](https://attack.mitre.org/techniques/T1018), and other discovery or [Credential Access](https://attack.mitre.org/tactics/TA0006) activity to support both ongoing and future campaigns.

Adversaries may collect various types of information about Wi-Fi networks from hosts. For example, on Windows names and passwords of all Wi-Fi networks a device has previously connected to may be available through `netsh wlan show profiles` to enumerate Wi-Fi names and then `netsh wlan show profile “Wi-Fi name” key=clear` to show a Wi-Fi network’s corresponding password.(Citation: BleepingComputer Agent Tesla steal wifi passwords)(Citation: Malware Bytes New AgentTesla variant steals WiFi credentials)(Citation: Check Point APT35 CharmPower January 2022) Additionally, names and other details of locally reachable Wi-Fi networks can be discovered using calls to `wlanAPI.dll` [Native API](https://attack.mitre.org/techniques/T1106) functions.(Citation: Binary Defense Emotes Wi-Fi Spreader)

On Linux, names and passwords of all Wi-Fi-networks a device has previously connected to may be available in files under ` /etc/NetworkManager/system-connections/`.(Citation: Wi-Fi Password of All Connected Networks in Windows/Linux) On macOS, the password of a known Wi-Fi may be identified with ` security find-generic-password -wa wifiname` (requires admin username/password).(Citation: Find Wi-Fi Password on Mac)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Agent Tesla
* Emotet

## APTs (Intrusion Sets)

* Magic Hound