System Network Configuration Discovery: Wi-Fi Discovery, Sub-technique T1016.002 - Enterprise

Archived: 2026-04-05 17:14:11 UTC

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, Remote System Discovery, and other discovery or Credential Access 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.[1][2][3] Additionally, names and other details of locally reachable Wi-Fi networks can be discovered using calls to `wlanAPI.dll` Native API functions.[4]

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/`.[5] On macOS, the password of a known Wi-Fi may be identified with `security find-generic-password -wa wifiname` (requires admin username/password).[6]

Source: https://attack.mitre.org/techniques/T1016/002