Adversary-in-the-Middle, Technique T1557 - Enterprise

Archived: 2026-04-05 17:27:13 UTC

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.[1]

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.[2][3][4] Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens (Steal Application Access Token) and session cookies (Steal Web Session Cookie).[5][6] Downgrade Attacks can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.[7][8][9]

Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in Transmitted Data Manipulation. Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to Impair Defenses and/or in support of a Network Denial of Service.

Source: https://attack.mitre.org/techniques/T1557