# TTP Detail – T1557

## TTP Information

Name: Adversary-in-the-Middle

Description: 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](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). 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.(Citation: Rapid7 MiTM Basics)  
  
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.(Citation: ttint\_rat)(Citation: dns\_changer\_trojans)(Citation: ad\_blocker\_with\_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens ([Steal Application Access Token](https://attack.mitre.org/techniques/T1528)) and session cookies ([Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)).(Citation: volexity\_0day\_sophos\_FW)(Citation: Token tactics) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s 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.(Citation: mitm\_tls\_downgrade\_att)(Citation: taxonomy\_downgrade\_att\_tls)(Citation: tlseminar\_downgrade\_att)  
  
Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

## Threat-Mapped Scoring

Score: 3.15

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: collection

## Malware

* Dok
* Line Runner

## Tools

* NPPSPY

## APTs (Intrusion Sets)

* Kimsuky
* Sea Turtle