# TTP Detail – T1557.002

## TTP Information

Name: ARP Cache Poisoning

Description: Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002).

The ARP protocol is used to resolve IPv4 addresses to link layer addresses, such as a media access control (MAC) address.(Citation: RFC826 ARP) Devices in a local network segment communicate with each other by using link layer addresses. If a networked device does not have the link layer address of a particular networked device, it may send out a broadcast ARP request to the local network to translate the IP address to a MAC address. The device with the associated IP address directly replies with its MAC address. The networked device that made the ARP request will then use as well as store that information in its ARP cache.

An adversary may passively wait for an ARP request to poison the ARP cache of the requesting device. The adversary may reply with their MAC address, thus deceiving the victim by making them believe that they are communicating with the intended networked device. For the adversary to poison the ARP cache, their reply must be faster than the one made by the legitimate IP address owner. Adversaries may also send a gratuitous ARP reply that maliciously announces the ownership of a particular IP address to all the devices in the local network segment.

The ARP protocol is stateless and does not require authentication. Therefore, devices may wrongly add or update the MAC address of the IP address in their ARP cache.(Citation: Sans ARP Spoofing Aug 2003)(Citation: Cylance Cleaver)

Adversaries may use ARP cache poisoning as a means to intercept network traffic. This activity may be used to collect and/or relay data such as credentials, especially those sent over an insecure, unencrypted protocol.(Citation: Sans ARP Spoofing Aug 2003)

## Threat-Mapped Scoring

Score: 3.05

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: collection

## APTs (Intrusion Sets)

* Cleaver
* LuminousMoth