Man-in-the-middle attack

By Kaspersky

Published: 2017-08-10 · Archived: 2026-04-06 01:27:41 UTC

During a **man-in-the-middle (MitM) attack**, threat actors gain access to a communication channel between legitimate parties (such as users, applications or network devices), allowing the perpetrators to view, delete or modify any message sent.

Man-in-the-middle attack mechanism

There are different ways to gain access to a communication channel. For example, an unscrupulous post office employee might exploit their position to open letters and parcels (an offline MitM attack).

With regard to network communications that attackers do not have access to by default, they can:

- Hack a service or device that does have access – such as a router.
- Mimic a legitimate participant in the information exchange, such as an app, website, VPN server or access point.

Attackers can use the following methods to direct victims' traffic through their own resources:

- Using fake access points: attackers create passwordless Wi-Fi access points and/or access points with names similar to legitimate ones. If victims unwittingly connect to these, all their internet traffic will pass through the attackers' device.
- ARP spoofing (ARP poisoning): attackers broadcast over the local network the mapping between the IP address of a legitimate device and the MAC address of their own device. This attack is opted for if the perpetrators have access to the victim's local network.
- DNS spoofing: attackers change the DNS cache (records that map domain names (website addresses) to the IP addresses of the servers on which these sites are located) on a router or vulnerable DNS server, mapping domain names to attacker-controlled IP addresses. If users try to open the corresponding site in their browser, they are directed to a malicious copy that is often indistinguishable from the original.
- URL spoofing: attackers create fake resources with URL addresses similar to those of legitimate sites. If a user opens the fake site instead of the legitimate one, the attackers can act as an intermediary between the user and the legitimate site.

Why man-in-the-middle attacks are dangerous

An attacker with full access to a victim's communication channel can:

- Read, modify and delete messages.
- Steal confidential information such as payment card details, account credentials and correspondence.
- View, delete and spoof files, including substituting downloadable apps with malicious versions.

Related products

Kaspersky Premium
Kaspersky VPN
Kaspersky Fraud prevention

Related Posts
