digital hands®

Intercepted:

How MDR Protects Your Business from Man-in-the-Middle (MitM) Attacks

Part 5 of a 7 part series

Table of Contents

Why Every CISO and SOC Should Care About MitM Attacks 03

How a MitM Attack May Unfold 04

How to Combat MitM Attacks with Managed Detection and Response Services 05

Benefits of MDR Beyond Man-in-the-Middle Defense 06

Man-in-the-middle (MitM), also known as adversary-in-the-middle (AitM) attacks are used to intercept and potentially tamper with communications between two parties — essentially inserting themselves between users and trusted parties like legitimate websites or services. These attacks are common for executing malicious activities such as stealing logins or session cookies, manipulating data to compromise transactions or deceive users, gathering intelligence for espionage purposes, or disrupting operations. **Some common MitM techniques include:**

- MFA bypass — Bad actors redirect users to a fake identity-as-a-service (IdaaS) website to harvest login credentials, then use so-called 2FA-pass-on techniques to input the credentials into the legitimate IdaaS provider's website to trigger an MFA request and trick the user into accepting it.
- Zero-days on edge devices – Bad actors could exploit a zero-day vulnerability on the edge devices and then redirect traffic, intercept traffic, and change policies to allow unauthorized internal and external access into the customer's network.
- Wi-Fi eavesdropping — the bad actors create a fake, malicious Wi-Fi network, often with a legitimate sounding name like a local business.
- DNS spoofing — also known as DNS cache poisoning, this attack manipulates DNS records to redirect users to a spoofed version of a trusted website.
- Session hijacking — attackers steal active web session cookies or tokens to take over a user's account without friction.
- HTTPS spoofing — users are secretly redirected from an HTTPS link to a nonsecure HTTP website to allow threat actors to steal data or track user interactions with the site.

Why Every CISO and SOC Should Care About MitM Attacks

MitM attacks can have huge implications. One of the most eye-opening examples was the 2017 Equifax data breach, when attackers exploited a vulnerability in the open-source web application framework Apache Struts to deploy a malicious Java application that masqueraded as a legitimate Equifax tool. The data breach cost the company $700 million in damages and compromised sensitive data (including Social Security numbers and birthdates) of 147.7 million U.S. consumers — nearly half of the country's population.

MitM attacks are difficult to detect and don't raise any red flags for the users. Yet they're easy to execute, making them a preferred technique.

The risk of MitM attacks is high for any organization:

- ✓ 69% of surveyed individuals use public Wi-Fi at least once a week, and nearly half of them say they do it even when unsure if the network is legit.
- ✓ 40% of people who used public Wi-Fi said they've had their data compromised.
- ✓ Nearly a quarter of surveyed organizations have experienced an MitM attack in the past year.
- ✓ 30% of organizations experienced a DNC spoofing attack in 2023, up from 25% in 2022.

How a MitM Attack May Unfold

The adversary's techniques varies depending on the type of attack, but here's what a typical DNS spoofing attack may look like:

STEP 1

Intercepting DNS requests

Attackers compromise a DNS server's cache (e.g., by exploiting a vulnerability) and insert an unauthorized domain name or IP into the cache, manipulating the server to redirect queries to the spoofed website.

STEP 2

Capturing user credentials

The unwitting users enter their login credentials, which are then captured by the cybercriminals.

STEP 3

Exploitation

The fraudsters use the stolen credentials to access the user accounts to infiltrate an organization or conduct fraudulent transactions.

For example, attackers create a fraudulent but authentic looking replica of a bank's website and through DNS spoofing, redirect the institution's customers to the malicious site. Once the customers log in, the attackers capture login details. They then take over the customer accounts to siphon funds or perform other fraudulent activities.

How to Combat MitM Attacks with Managed Detection and Response Services

MDR can help contain these attacks to limit their impact, spread, and severity. **Here's what the playbook may look like, using a combination of automated tools and human experts:**

1. Detection

The MDR's detection platform sees across multiple technologies. This breadth and depth across systems allows it to detect abnormal behaviors that single point systems may miss due to the lack of curated threat intelligence and AI capabilities. The platform monitors communication patterns to identify anomalies such as:

- Suspicious SSL/TLS traffic behavior (e.g., mismatched certificates)
- Unexpected IP routing changes or DNS resolution activities
- Unauthorized configuration changes to your firewall
- Abnormal network traffic flows that may indicate eavesdropping attempts

2. Automation

The MDR platform's automated workflows isolate the systems that are communicating with known malicious IPs or DNS servers to prevent further data interceptions. The platform also triggers certificate revocations to prevent attackers from spoofing legitimate sites.

3. Investigation

MDR analysts investigate the flagged anomalies by reviewing network logs to determine whether communications have been intercepted or manipulated. They also assess whether MitM activity is part of a broader attack like malware deployment.

4. Action

The MDR partner invalidates exposed credentials and enforces MFA. Analysts guide remediation steps, such as securing DNS configurations or patching SSL/TLS vulnerabilities. MDR threat hunters use threat intelligence along with other techniques to proactively search for other suspicious activities and anomalies that are completely unknown and may not have been detected by automated means.

Benefits of MDR beyond man-in-the-middle defense

Digital Hands' Real-World MDR offers much more than defense against MitM attacks.

Your MDR partner can augment your in-house SOC or security team, enabling them to:

- ✓ See more — faster — to protect your environment holistically.
- ✓ Get higher-fidelity alerts and integrated, enriched telemetry.
- ✓ Improve operational efficiency while allowing you to automate your workflows based on your risk appetite.
- ✓ Increase response time with automated containment and expert-led investigations, reducing the window of opportunity for the adversary.

Buyer's Guide

Not sure where to start?

Get your MDR Buyer's Guide to understand key evaluation criteria and the 8 must-ask questions before you buy.

Download Now