FORGE

The Arkansas Cyber Defense Center

Man in the Middle Attack

In this type of attack, the perpetrator positions themself in a conversation between a user and an application in order to impersonate one of the parties or eavesdrop to gain information.

What do threat actors want?
The goal of this attack is to steal information (login credentials, credit card numbers, etc.). Additionally, it can be used to gain access to a secured network perimeter.

Tactics of this kind of attack:
IP Spoofing: Altering packet headers to disguise an IP address
DNS spoofing: Altering a website's address record in order to catch the websites incoming traffic
ARP spoofing: Linking the attacker's MAC address to the IP address of a legitimate user on a LAN to get access to the user's traffic.

Prevention:
- Avoid using WiFi that isn't password protected.
- Heed the warnings of browser notifications saying the website is unsecure.
- Log out of applications that aren't in use.
- Avoid public networks.

REPORT A CYBER INCIDENT:

forge.institute/acdc
501-239-9599