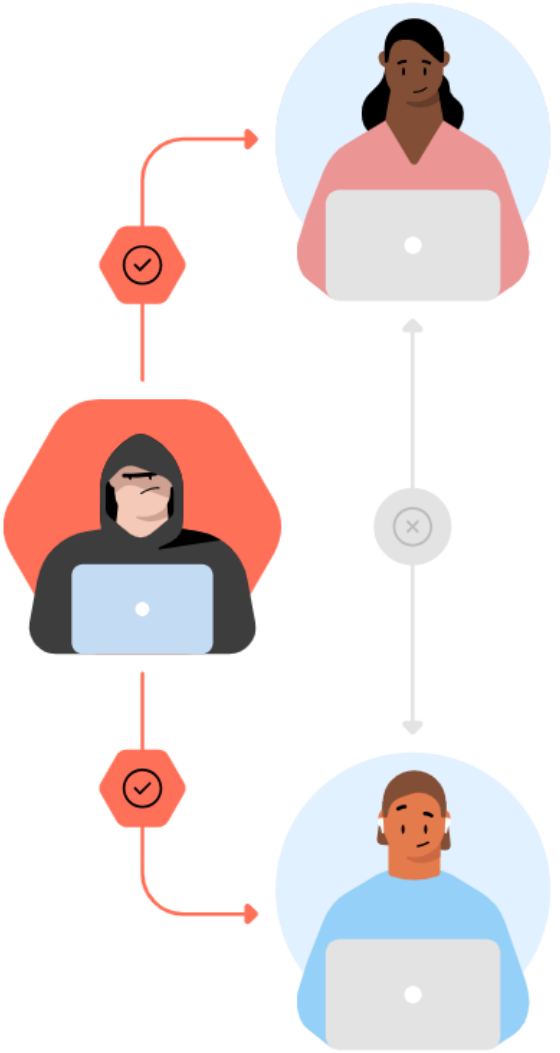
Redes de Computadores

Ataques Man-in-the-middle (MITM)

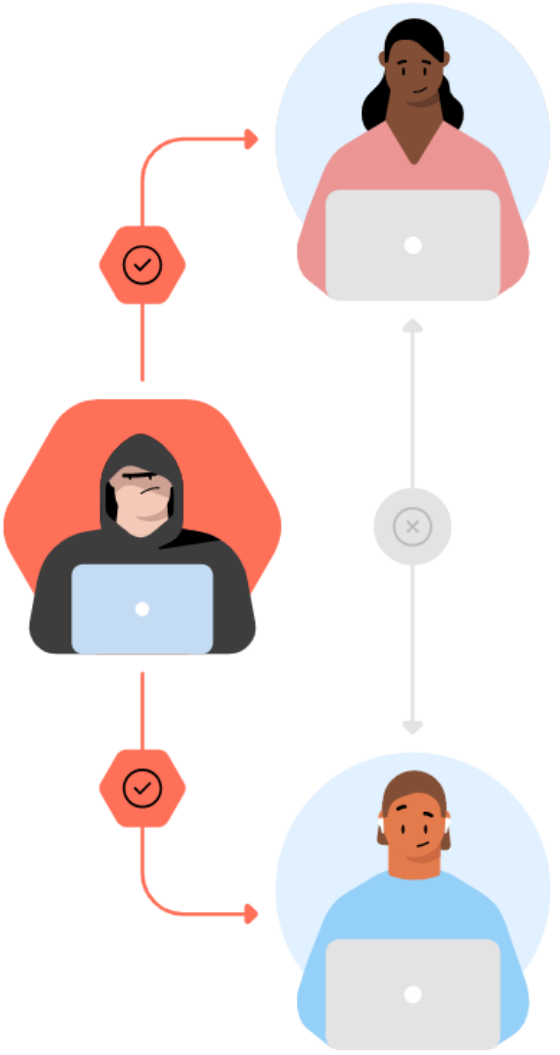
O que é?

É um ataque onde o invasor se posiciona entre duas partes que acreditam estar se comunicando diretamente para **interceptar** e consequentemente **ler**, **modificar** ou **injetar dados**.



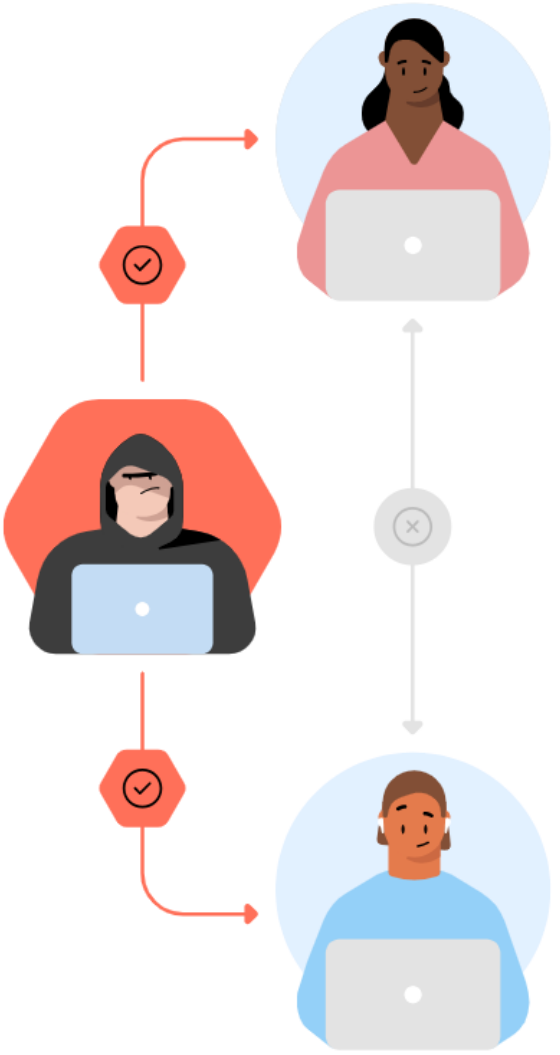
Tipos Comuns

- **ARP Spoofing**
- DNS Spoofing
- IP Spoofing
- HTTPS / SSL Hijacking
- Evil Twin (Rede falsa)



O que é ARP?

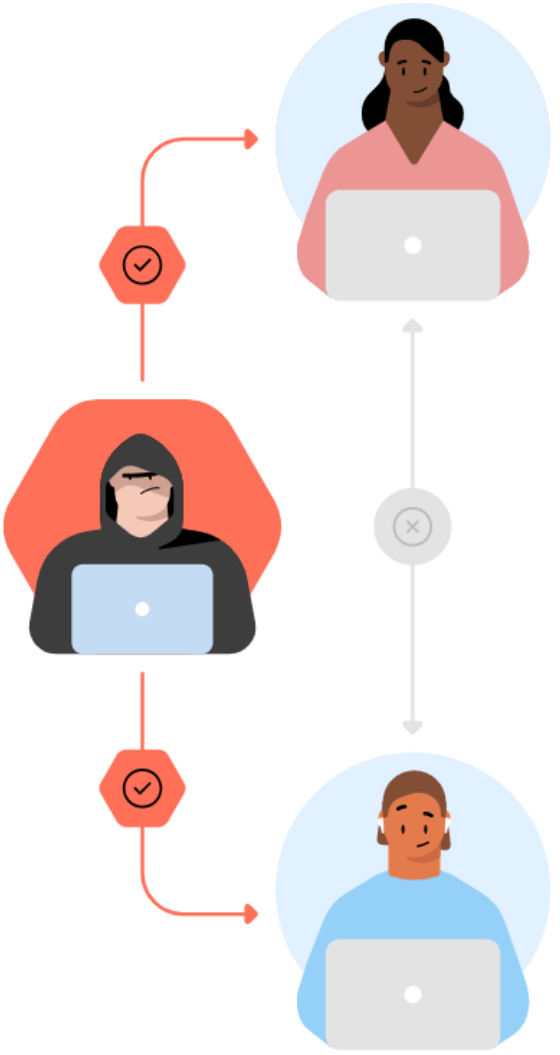
O ARP é um protocolo que tem como objetivo mapear um **endereço de IP** a um **endereço MAC** em uma rede local (LAN)



Como funciona?

Para comunicar localmente, um dispositivo envia uma requisição (ARP Request) em broadcast solicitando o endereço MAC de um determinado IP.

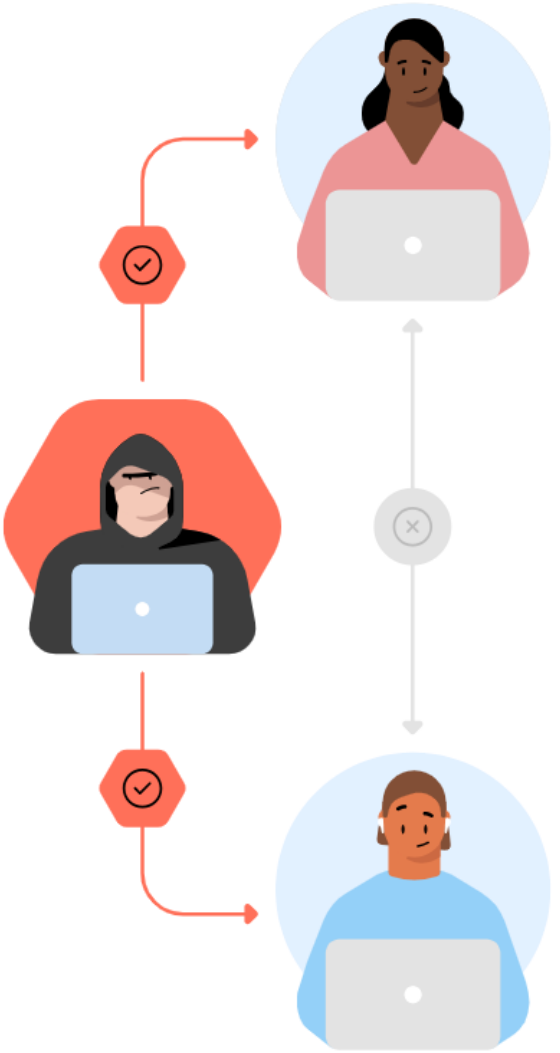
O dispositivo com o IP correspondente responde com seu endereço MAC (ARP Reply).



Como é feito o ataque?

O ARP é um protocolo "confiável" por padrão, ou seja, ele não possui mecanismos de autenticação para verificar a legitimidade de uma resposta ARP.

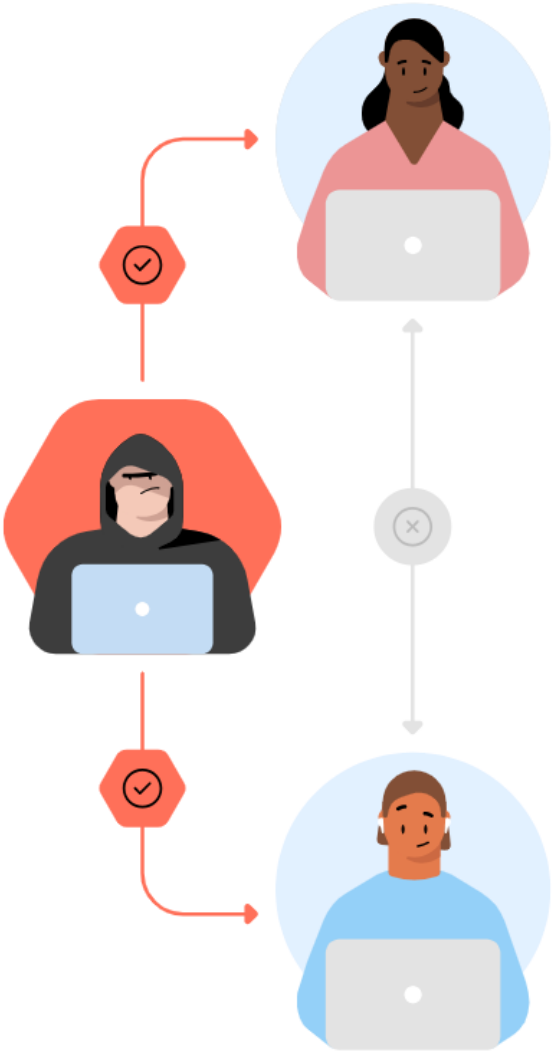
O ataque explora essa falta de autenticação no protocolo ARP.



Como é feito o ataque?

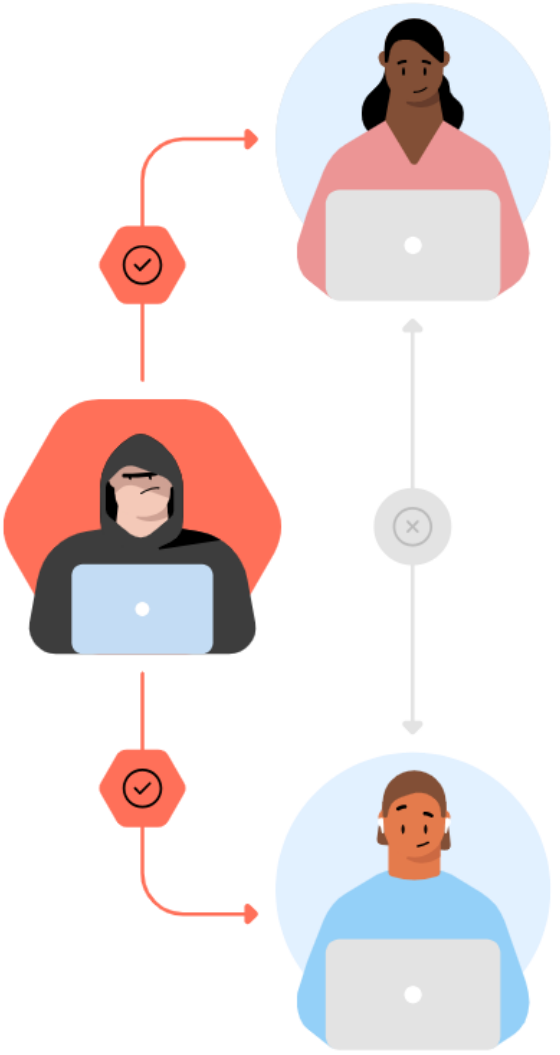
O atacante utiliza ferramentas de monitoramento de rede para identificar os dispositivos conectados e envia pacotes ARP dizendo que o **IP do Roteador** e o **IP da vítima** estão associados ao seu **MAC**.

Resultado: Ambos enviam seus pacotes para o atacante!



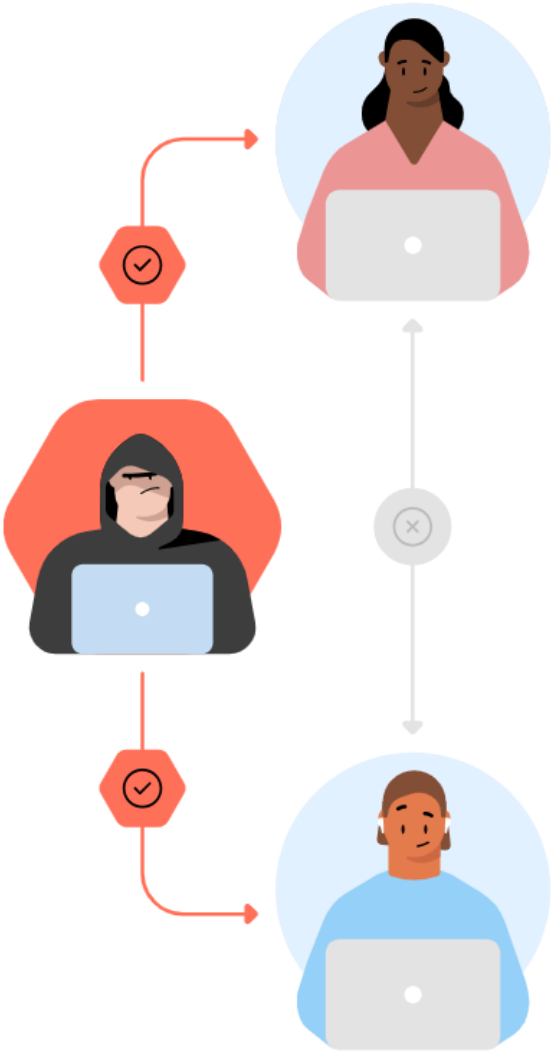
Como é feito o ataque?

Para se mascarar e não ser detectado, o atacante encaminha os pacotes corretamente para o destino real.



Consequências

- Roubo de senhas, cookies e dados sensíveis.
- Redirecionamento de tráfego para sites falsos.
- Interrupção de serviços (DoS)



Como se proteger

- Conexões Seguras
  - HTTPS / VPN
- DHCP Snooping
- DAI (Dynamic ARP Inspection)
- Vínculo IP-MAC fixo