1.Ataques *on path*

Os ataques on-path, também conhecidos como man-in-the-middle (MITM), permitem que um invasor se posicione entre dois dispositivos e monitore todo o tráfego trocado entre eles. O atacante pode não apenas visualizar os dados que estão sendo transmitidos, mas também modificá-los em tempo real, sem que as partes envolvidas percebam. Como o ataque ocorre de forma transparente, a vítima continua a interagir normalmente, sem suspeitar que suas informações podem estar sendo interceptadas e manipuladas.

Uma das formas mais comuns desse ataque é o **ARP poisoning**, que ocorre dentro de uma mesma rede local. Como o protocolo ARP (**Address Resolution Protocol**) não possui mecanismos de autenticação ou criptografia, ele pode ser facilmente manipulado. Quando um dispositivo deseja se comunicar com outro dentro da rede, ele primeiro envia um pedido ARP solicitando o endereço MAC associado a um determinado IP. O dispositivo de destino responde com seu endereço MAC correto, permitindo a comunicação direta. No entanto, um atacante pode interceptar essa solicitação e responder com um endereço MAC falso, redirecionando o tráfego para si próprio antes de encaminhá-lo ao destino legítimo. Dessa forma, todo o tráfego entre um computador e o roteador passa pelo atacante, que pode analisar, modificar ou bloquear os pacotes conforme desejar.

Além dos ataques baseados em rede, existe uma variante chamada **on-path browser attack**, também conhecida como **Man-in-the-Browser (MITB)**. **Nesse caso, o malware é instalado diretamente no dispositivo da vítima, funcionando como um proxy dentro do navegador**. Como o ataque ocorre no próprio sistema do usuário, ele pode capturar todas as informações digitadas, incluindo credenciais bancárias e senhas, mesmo que o tráfego esteja criptografado. O malware pode até modificar as transações antes que sejam enviadas ao banco, transferindo valores para contas controladas pelos atacantes sem que a vítima perceba.

Esses ataques são extremamente perigosos porque exploram a confiança do usuário na comunicação segura. Enquanto um MitM tradicional pode ser mitigado por criptografia de ponta a ponta, um ataque MITB consegue contornar essa proteção, pois a captura acontece antes dos dados serem criptografados. Isso significa que, mesmo acessando um site seguro com HTTPS, a ameaça ainda pode roubar informações confidenciais.

A melhor defesa contra esses ataques envolve a adoção de múltiplas camadas de segurança. Para evitar ARP poisoning, é recomendável utilizar **ARP Spoofing Detection**, segmentação de redes e protocolos mais seguros, como IPv6, que possui mecanismos de proteção contra esse tipo de manipulação. Já para evitar ataques **Man-in-the-Browser**, é fundamental manter sistemas operacionais e navegadores sempre atualizados, utilizar soluções antivírus avançadas e ativar autenticação

multifator para evitar que credenciais comprometidas sejam suficientes para permitir acesso não autorizado. Com medidas de segurança adequadas, é possível reduzir significativamente os riscos de interceptação e manipulação de dados em redes e dispositivos.

2.Ataques *on path*: spoofing - Extras

É um ataque de representação e tira o proveito de uma relação de confiança entre dois sistemas. Se ambos aceitarem a autenticação de cada um deles, um indivíduo conectado a um sistema pode não passar novamente pelo processo de autenticação novamente para acessar outros sistemas. Um invasor pode se aproveitar desse arranjo, enviando um pacote para um sistema que parece ter vindo de um sistema confiável. Existem vários tipos de ataques de spoofing como os de endereço MAC, endereço IP, spoofing ARP e spoofing DNS.

Se os atores da ameaça comprometer muitos hosts, eles podem iniciar um ataque DDoS, ataques semelhantes, porém com aumento na magnitude pois se origina de diversas fontes de forma coordenada. Alguns dos termos utilizados neste tipo de ataque são os zumbis, grupo de hosts comprometidos (agentes) por um worm; bots, malware projetado para infectar um host e se comunicar com um sistema; handler, se referindo ao servidor primário de comando e controle, responsável pelos zumbis ou a própria botnet; botnet, referindo-se a todos os hosts infectados pelo worm controlador.

3.Ataques *on path*: MitM - Extras

Um ataque MitM ocorre quando os agentes da ameaça se posicionam entre a origem e o destino. Agora eles podem monitorar, capturar e controlar ativamente a comunicação de forma transparente.

4.Ataques *on path*: MitMO - Extras

Man-in-the-Mobile é uma variação onde se assume o controle de um dispositivo móvel. O dispositivo infectado envia as informações confidenciais do usuário para os invasores. Um ataque de repetição ocorre quando um invasor captura uma parte de uma comunicação entre dois hosts e retransmite a mensagem capturada mais tarde. Os ataques de repetição driblam os mecanismos de autenticação.