1.Ataques DNS

O sistema de nomes de domínio, conhecido como DNS, é fundamental para a navegação na internet, pois converte nomes de sites amigáveis, como professormesser.com, em endereços IP utilizáveis pelos computadores. No entanto, esse mecanismo pode ser explorado por atacantes por meio de técnicas de **envenenamento de DNS (DNS poisoning), que redirecionam usuários para sites falsos sem que percebam**. Algumas dessas estratégias envolvem a modificação direta do servidor DNS, mas como esses servidores costumam ser bem protegidos, esse tipo de ataque não é o mais comum. Métodos mais acessíveis incluem a alteração do arquivo de hosts local no computador da vítima. Para que isso aconteça, o invasor precisa obter acesso ao sistema com privilégios administrativos, modificando esse arquivo que contém uma lista de domínios e seus respectivos endereços IP. Assim, sempre que o usuário tentar acessar um site, seu próprio computador usará as informações desse arquivo em vez de consultar um servidor DNS legítimo.

Outra abordagem explorada pelos criminosos é a interceptação de requisições DNS em tempo real, também conhecida como ataque **Man-in-the-Middle** (MitM). **O invasor posiciona-se entre a comunicação do usuário e o servidor DNS e responde às consultas com endereços IP falsificados, direcionando a vítima para um site malicioso**. Essa técnica exige que o atacante tenha acesso à rede da vítima, o que pode ser feito explorando vulnerabilidades em conexões públicas de Wi-Fi ou roteadores desprotegidos.

Quando um invasor compromete um servidor DNS, ele pode modificar registros para redirecionar o tráfego de qualquer domínio para um endereço de sua escolha. Suponha que um hacker obtenha acesso a um servidor DNS e altere o endereço IP de professormesser.com para o IP de um servidor controlado por ele. Qualquer usuário que tentar acessar esse site será automaticamente redirecionado para a página falsa, onde o atacante pode coletar credenciais de login, informações bancárias ou instalar malware no dispositivo da vítima.

Um caso real de ataque desse tipo ocorreu em 22 de outubro de 2016, quando criminosos modificaram 36 domínios de um banco brasileiro, alterando os registros DNS associados a desktops, dispositivos móveis e outros sistemas utilizados pelos clientes. Durante seis horas, todas as requisições desses domínios foram redirecionadas para servidores maliciosos, permitindo que os atacantes coletassem informações financeiras e dados de login dos clientes da instituição. O banco não divulgou detalhes sobre o ataque, mas estima-se que milhões de clientes possam ter sido afetados.

Outro método utilizado para enganar usuários é o sequestro de URLs, conhecido como **URL hijacking** ou **typosquatting**. **Essa técnica se aproveita de erros de digitação comuns para registrar domínios semelhantes aos de sites populares**. Por exemplo, um atacante pode registrar um domínio como

professormessers.com em vez de professormesser.com, adicionando uma letra extra para enganar usuários desatentos. Outra variação é utilizar um sufixo diferente, como .org em vez de .com, o que pode levar os visitantes a acreditarem que estão no site correto.

O objetivo do URL hijacking pode variar. Em alguns casos, o atacante pode simplesmente exibir anúncios para gerar receita com cliques. Em outros, ele pode tentar vender o domínio para o proprietário legítimo por um valor elevado. Há também situações mais perigosas, onde os sites falsos são usados para capturar credenciais de login ou distribuir malware, transformando dispositivos das vítimas em parte de uma botnet ou infectando-os com ransomware.

Para se proteger contra esses ataques, é essencial sempre verificar cuidadosamente os endereços de sites antes de inserir informações sensíveis. Além disso, evitar clicar em links enviados por e-mails suspeitos reduz o risco de ser redirecionado para páginas fraudulentas. Medidas como o uso de **DNS seguros e protegidos por criptografia**, autenticação multifator e softwares de segurança atualizados ajudam a minimizar os riscos e garantem uma navegação mais segura na internet.