O que é segurança de DNS?

O DNS não foi projetado com a segurança em mente e existem muitos tipos de ataques criados para explorar vulnerabilidades no sistema DNS.

Protegendo o DNS

Copiar o link do artigo

O que é segurança de DNS?

A segurança de DNS é a prática de proteger a infraestrutura de DNS contra ataques cibernéticos para mantê-la funcionando de forma rápida e confiável. Uma estratégia de segurança de DNS eficaz incorpora várias defesas sobrepostas, incluindo o estabelecimento de servidores de DNS redundantes, a aplicação de protocolos de segurança como DNSSEC e a exigência de registro de DNS rigoroso.

Por que a segurança de DNS é importante?

Como muitos protocolos da internet, o sistema de DNS não foi projetado com a segurança em mente e contém várias limitações de design. Essas limitações, combinadas com os avanços da tecnologia, tornam os servidores de DNS vulneráveis a um amplo espectro de ataques, incluindo falsificação, amplificação, DoS (Negação de Serviço) ou interceptação de informações pessoais privadas. E como o DNS é parte integrante da maioria das solicitações da internet, ele pode ser o principal alvo de ataques.

Além disso, os ataques de DNS são frequentemente implantados em conjunto com outros ataques cibernéticos para distrair as equipes de segurança do verdadeiro alvo. Uma organização precisa ser capaz de mitigar rapidamente os ataques de DNS para que não fique muito ocupada para lidar com ataques simultâneos por meio de outros vetores.

Quais são alguns dos ataques comuns

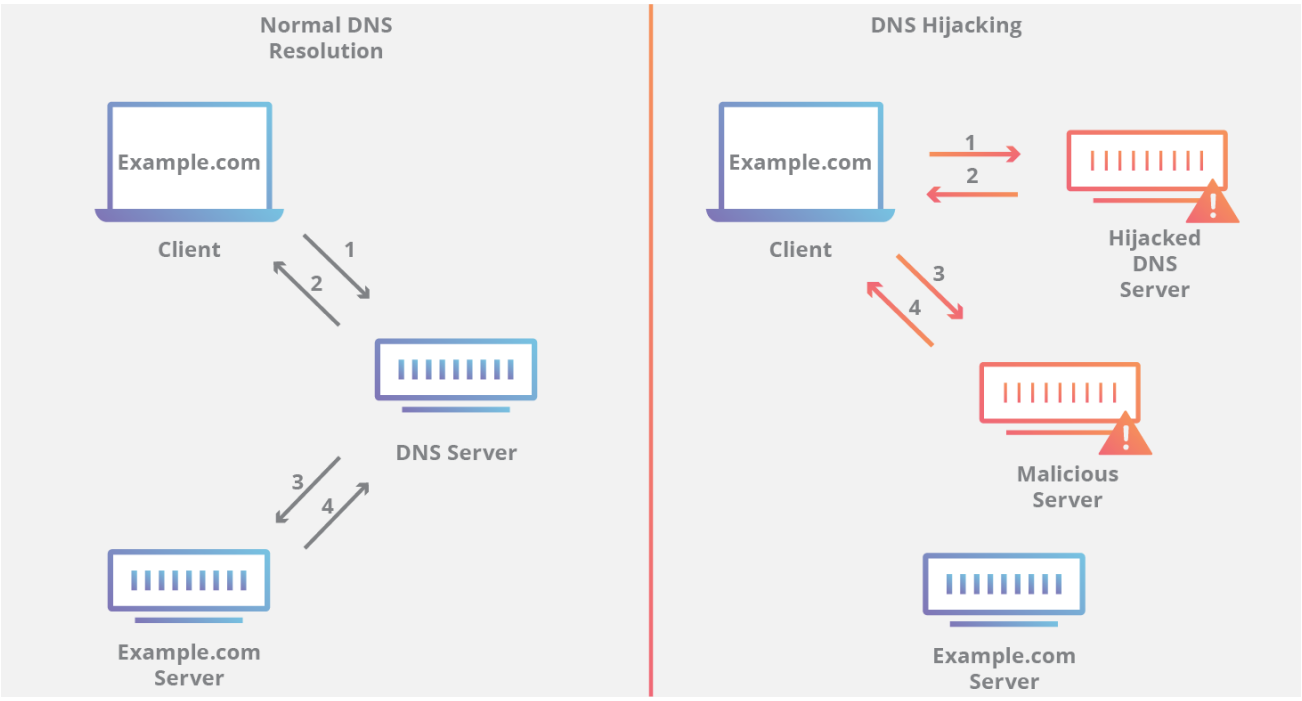
envolvendo o DNS?

Os invasores encontraram várias maneiras de direcionar e explorar servidores de DNS. Aqui estão algumas das mais comuns:

Falsificação de DNS/envenenamento de cache**:** trata-se de um ataque no qual dados de DNS forjados são introduzidos no cache de um resolvedor de DNS e, como resultado, o resolvedor retorna um endereço IP incorreto para um domínio. Ao invés de ir para o site correto, o tráfego pode ser desviado para uma máquina mal-intencionada ou para qualquer outro lugar que o invasor desejar; frequentemente, será uma réplica do site original usada para fins mal-intencionados, como a distribuição de malware ou a coleta de informações de login.

Tunelamento de DNS: esse ataque usa outros protocolos para criar um túnel que atravessa as consultas e respostas de DNS. Os invasores podem usar SSH, TCP ou HTTP para transmitir malware ou informações roubadas nas consultas de DNS sem serem detectados pela maioria dos firewalls.

Sequestro de DNS: no sequestro de DNS, o invasor redireciona as consultas para um nameserver de domínio diferente. Isso pode ser feito com malware ou por meio da modificação não autorizada de um servidor de DNS. Embora o resultado seja semelhante ao da falsificação de DNS, trata-se de um ataque fundamentalmente diferente, pois visa o registro de DNS do site no nameserver e não no cache de um resolvedor.



Ataque NXDOMAIN: trata-se de um tipo de ataque de inundação de DNS no qual um invasor inunda um servidor de DNS com solicitações perguntando por registros que não existem, na tentativa de causar uma negação de serviço para o tráfego legítimo. Isso pode ser feito usando ferramentas de ataque sofisticadas que podem autogerar subdomínios exclusivos para cada

solicitação. Os ataques NXDOMAIN também podem visar um resolvedor recursivo com o objetivo de encher seu cache com solicitações inválidas.

Ataque de domínio fantasma: um ataque de domínio fantasma tem um resultado semelhante ao de um ataque NXDOMAIN a um resolvedor de DNS. O invasor configura vários servidores de um domínio "fantasma" que não respondem às solicitações ou o fazem muito lentamente.

O resolvedor é então atingido por uma enxurrada de solicitações para esses domínios e fica paralisado à espera de respostas, acarretando uma performance lenta e a negação de serviço.

Ataque de subdomínio aleatório: nesse caso, o invasor envia consultas de DNS para vários subdomínios aleatórios inexistentes de um site legítimo. O objetivo é criar uma negação de serviço do nameserver autoritativo do domínio, impossibilitando as pesquisas no site a partir do nameserver. Como efeito colateral, o provedor que atende ao invasor também pode ser afetado, já que o cache do resolvedor recursivo ficará carregado de solicitações inválidas.

Ataque de bloqueio de domínio: os invasores orquestram essa forma de ataque configurando domínios e resolvedores especiais para criar conexões TCP com outros resolvedores legítimos. Quando os resolvedores visados enviam solicitações, esses domínios retornam fluxos lentos de pacotes aleatórios, paralisando os recursos do resolvedor.

Ataque de CPE baseado em botnet: esses ataques são realizados usando dispositivos de CPE (Equipamento no Local do Cliente, ou seja, hardware fornecido por provedores de serviços para uso de seus clientes, como modems, roteadores, caixas de cabos etc.). Os invasores comprometem os CPEs e os dispositivos se tornam parte de uma botnet usada para executar ataques de subdomínios aleatórios contra um site ou domínio.

O que é DNSSEC?

As Extensões de Segurança do DNS (DNSSEC) são um protocolo de segurança criado para mitigar esse problema. O DNSSEC protege contra ataques assinando os dados digitalmente para ajudar a garantir sua validade. Para garantir uma pesquisa segura, a assinatura deve ocorrer em todos os níveis do processo de pesquisa de DNS.

Esse processo de assinatura é semelhante a alguém que assina um documento legal com uma caneta: essa pessoa assina de uma forma exclusiva que ninguém consegue copiar, e um perito forense pode examinar a assinatura e confirmar se o documento foi realmente assinado por essa pessoa. Essas assinaturas digitais garantem que os dados não foram adulterados.

O DNSSEC implementa uma política hierárquica de assinatura digital em todas as camadas do DNS. Por exemplo, no caso de uma pesquisa do domínio "google.com", um servidor raiz de DNS assinaria uma chave para o nameserver .COM e, em seguida, o nameserver .COM assinaria uma chave para o nameserver autoritativo do google.com.

Embora uma segurança aprimorada seja sempre a melhor opção, o DNSSEC foi projetado para ser compatível com versões anteriores para garantir que as pesquisas tradicionais de DNS ainda sejam resolvidas corretamente, embora sem a segurança adicional. O DNSSEC foi criado para funcionar com outras medidas de segurança, como SSL/TLS, como parte de uma estratégia holística de segurança na internet.

O DNSSEC cria uma corrente de confiança vinculativa e duradoura que percorre todo o trajeto até a zona raiz. Essa corrente de confiança não pode ser comprometida em nenhuma camada do DNS, pois caso isso ocorra a solicitação ficará vulnerável a um ataque on-path.

Para fechar a cadeia de confiança, a própria zona raiz precisa ser validada (comprovadamente livre de adulterações ou fraudes) e isso é realmente feito usando intervenção humana. Curiosamente, naquilo que é chamado Cerimônia de Assinatura da Zona Raiz, pessoas selecionadas do mundo inteiro se reúnem para assinar o DNSKEY RRset da zona raiz de maneira pública e auditada.

Abaixo uma explicação mais detalhada de como o DNSSEC funciona >>>

Quais são outras formas de proteção contra ataques baseados em DNS?

Além do DNSSEC, um operador de uma zona de DNS pode tomar outras medidas para proteger seus servidores. O maior provisionamento de infraestrutura é uma estratégia simples para superar ataques DDoS. Simplificando, se seus nameservers puderem lidar com mais tráfego do que o esperado, será mais difícil para um ataque baseado em volume sobrecarregar seu servidor. As organizações podem fazer isso aumentando a capacidade total de tráfego de seus servidores de DNS, estabelecendo vários servidores de DNS redundantes e usando o balanceamento de carga para rotear solicitações de DNS para servidores íntegros quando um começa a ter uma performance ruim.

Outra estratégia ainda é um firewall de DNS.

O que é um DNS Firewall?

O DNS Firewall é uma ferramenta que pode fornecer diversos serviços de segurança e desempenho para servidores de DNS. Um DNS Firewall fica entre o resolvedor recursivo de um usuário e o nameserver autoritativo do site ou serviço que ele está tentando acessar. O firewall pode fornecer um serviço de Rate Limiting para desligar os invasores que estão tentando sobrecarregar o servidor. Se o servidor tiver um tempo de inatividade como

tentando sobrecarregar o servidor. Se o servidor tiver um tempo de inatividade como resultado de um ataque ou por qualquer outro motivo, o DNS Firewall poderá manter o site ou o serviço do operador funcionando ao fornecer respostas de DNS a partir do cache.

Além de seus recursos de segurança, um DNS Firewall pode também fornecer soluções de desempenho, como pesquisas de DNS mais rápidas e custos reduzidos de largura de banda para o operador de DNS. Saiba mais sobre o DNS Firewall da Cloudflare.

O DNS como uma ferramenta de segurança

Os resolvedores de DNS também podem ser configurados para fornecer soluções de segurança para seus usuários finais (pessoas que navegam na internet). Alguns resolvedores de DNS fornecem recursos como a filtragem de conteúdo, que pode bloquear sites conhecidos por distribuírem malware e spam e a proteção contra botnets, que bloqueia a comunicação com botnets conhecidas. Muitos desses resolvedores de DNS seguros são de uso gratuito e um usuário pode se transferir para um desses serviços de DNS recursivo alterando uma única configuração em seu roteador local. O DNS da Cloudflare enfatiza a segurança.

As consultas de DNS são privadas?

Outra questão importante da segurança de DNS é a privacidade do usuário. As consultas de DNS não são criptografadas. Mesmo que os usuários usem um resolvedor de DNS como 1.1.1.1 que não rastreia suas atividades, as consultas de DNS trafegam pela internet em texto não criptografado. Isso significa que qualquer pessoa que interceptar a consulta pode ver quais sites o usuário está visitando.

Essa falta de privacidade tem impacto na segurança e, em alguns casos, nos direitos humanos; se as consultas de DNS não forem privadas, então se torna mais fácil para os governos censurar a internet e para os invasores espionarem o comportamento on-line dos usuários.

DNS sobre TLS e DNS sobre HTTPS são dois padrões para criptografar consultas de DNS para evitar que partes externas possam lê-las.

A Cloudflare oferece segurança de DNS

Os serviços de DNS da Cloudflare vêm com uma ampla variedade de recursos de segurança integrados, incluindo DNSSEC, mitigação de DDoS, funcionalidade multi-DNS e balanceamento de carga.

CONTEÚDO RELACIONADO

O que é DNS?

Tipos de servidor de DNS

DNS Round-Robin

Registro DNS CNAME

Registros DNS

Quer saber mais?

Inscreva-se para receber artigos de aprendizado sobre segurança da Cloudflare.

Assine

As informações que você fornece à Cloudflare são regidas pelos termos da nossa Política de Privacidade.