O que é envenenamento de cache DNS? | Falsificação de DNS

Os invasores podem envenenar um cache de DNS, fazendo com que os resolvedores de DNS façam o cache de informações falsas, resultando no resolvedor enviando o endereço IP errado aos clientes, e os usuários que tentam navegar em um site são direcionados para o local errado.

Protegendo o DNS

Copiar o link do artigo

O que é envenenamento do cache de DNS?

Imagine que, como um trote de calouros, os alunos do último ano do ensino médio mudem todos os números das salas de aula da escola para que os novos alunos chegando ao campus, que não ainda conhecem o layout do local, passem o dia inteiro perdidos e comparecendo às salas erradas. Agora imagine que os números de salas trocados sejam registrados em um diretório do campus e os alunos continuem indo para as salas erradas, até que alguém, finalmente, perceba o erro e corrija o diretório.

O envenenamento de cache de DNS é o ato de inserir informações falsas em um cache de DNS para que as consultas de DNS retornem uma resposta incorreta e os usuários sejam direcionados aos sites errados. O envenenamento de cache de DNS também é conhecido como "falsificação de DNS". Os endereços IP são os "números dos quartos" da internet, permitindo que o tráfego da web chegue aos lugares certos. Os caches dos resolvedores de DNS são o "catálogo do campus" e, quando armazenam informações defeituosas, o tráfego vai para os lugares errados até que as informações armazenadas em cache sejam corrigidas. (Observe que, na verdade, isso não desconecta os sites reais de seus endereços IP reais.)

Devido ao fato de que, geralmente, não há um jeito de os resolvedores de DNS verificarem os dados em seus caches, as informações de DNS incorretas permanecem no cache até que sua vida útil (TTL) expire ou sejam removidas manualmente. Algumas vulnerabilidades tornam o envenenamento de DNS possível, mas o principal problema é que o DNS foi desenvolvido para uma internet muito menor e baseado em um princípio de confiança (bem semelhante ao BGP). Existe um protocolo DNS mais seguro, denominado DNSSEC, que visa a solucionar alguns

Existe um protocolo DNS mais seguro, denominado DNSSEC, que visa a solucionar alguns desses problemas, mas que ainda não foi amplamente adotado.

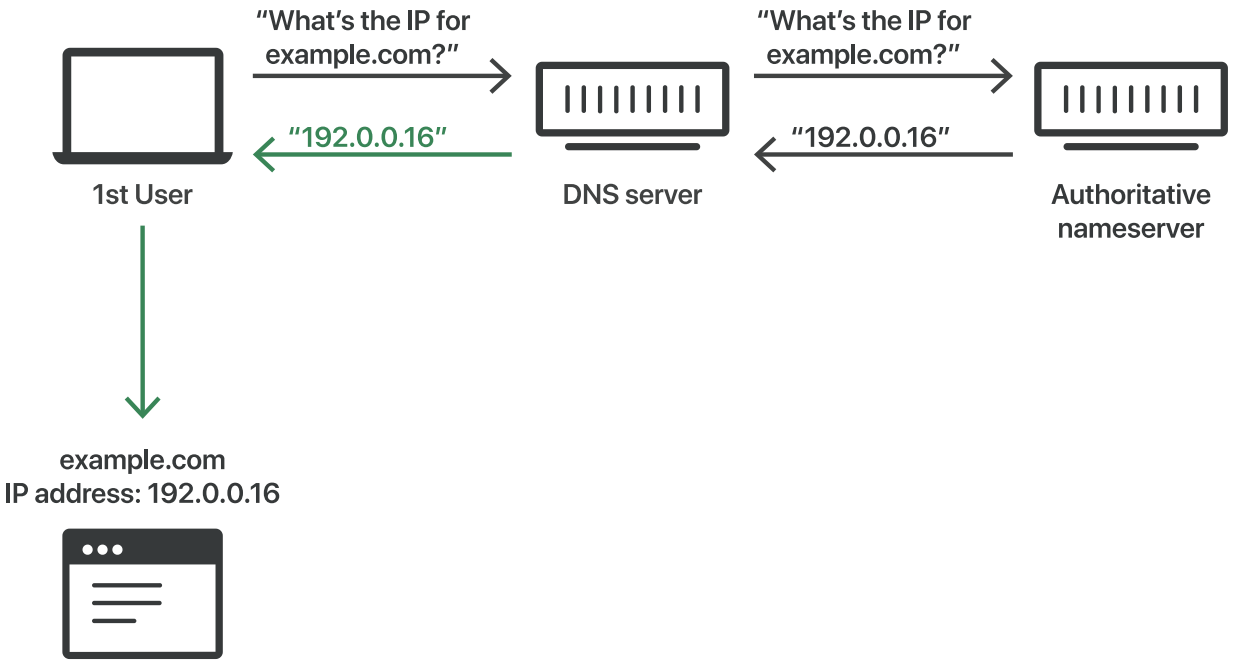
O que fazem os resolvedores de DNS?

Os resolvedores de DNS fornecem aos clientes um endereço IP associado a um nome de domínio. Em outras palavras, pegam os endereços de sites legíveis por humanos, como "cloudflare.com" e os convertem em endereços IP legíveis por máquina. Quando um usuário tenta navegar para um site, seu sistema operacional envia uma solicitação para um resolvedor de DNS. O resolvedor de DNS responde com o endereço IP e o navegador da internet pega esse endereço e inicia o carregamento do site.

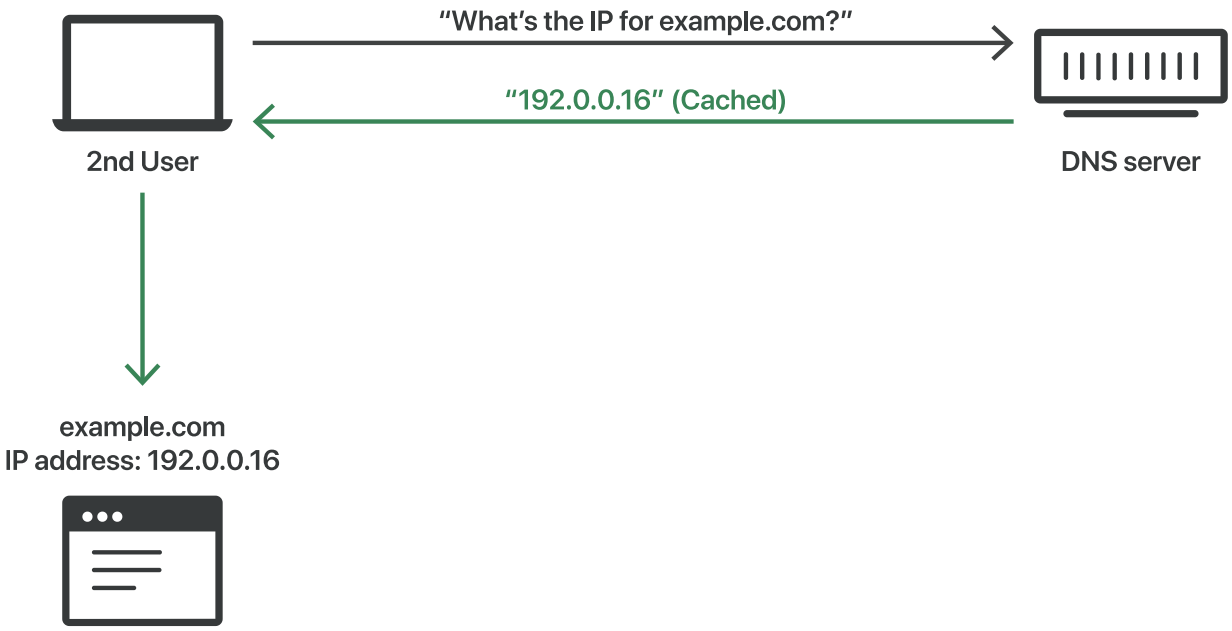
Como funciona o cache de DNS?

Um resolvedor de DNS salva as respostas a consultas de endereço IP por um determinado período de tempo. Assim, o resolvedor pode responder a consultas futuras muito mais rapidamente, sem precisar se comunicar com os diversos servidores envolvidos no processo típico de resolução de DNS. Os resolvedores de DNS salvam as respostas em seu cache enquanto a TTL (vida útil) designada associada a esse endereço IP permitir.

Resposta do DNS sem cache:



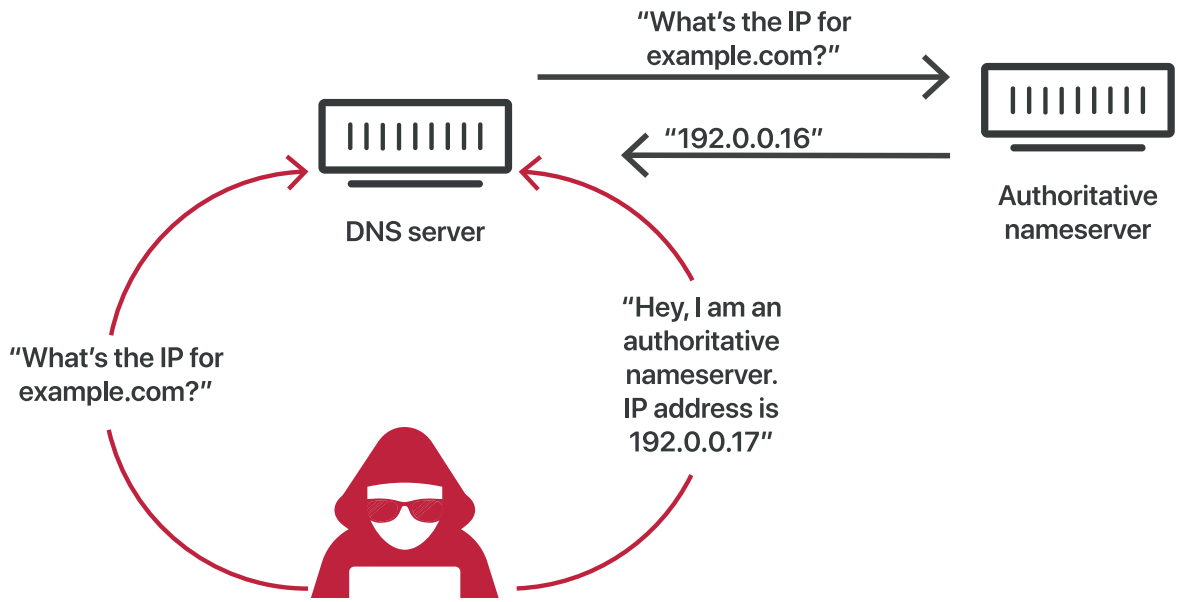
Resposta do DNS com cache:



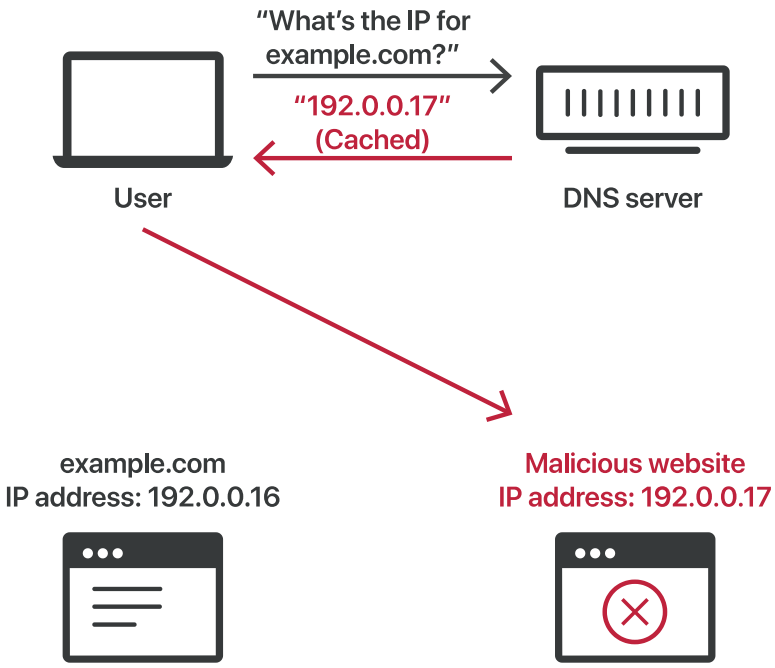
Como os invasores envenenam os caches de DNS?

Os invasores podem envenenar os caches de DNS representando o papel de nameservers de DNS, fazendo uma solicitação para um resolvedor de DNS e, em seguida, forjando a resposta quando o resolvedor de DNS consulta um nameserver. Isso é possível porque os servidores DNS usam o protocolo UDP ao invés do TCP, e também porque, atualmente, não existe uma verificação das informações de DNS.

Processo de envenenamento do cache de DNS:



Cache de DNS envenenado:



Ao invés de usar o protocolo TCP, que exige que ambas as partes envolvidas na comunicação executem um "aperto de mão" (handshake) para iniciar a comunicação e verificar a identidade dos dispositivos, as solicitações e respostas de DNS usam o UDP, ou Protocolo de Datagrama do Usuário. Com o UDP, não há garantias de que uma conexão esteja aberta, o destinatário esteja pronto para receber ou o remetente seja quem ele diz que é. Por esse motivo, o UDP é vulnerável à falsificação — um invasor pode enviar uma mensagem via UDP fingindo que é uma resposta de um servidor legítimo falsificando os dados do cabeçalho.

Se um resolvedor de DNS receber uma resposta falsificada, ele aceita e armazena os dados em

cache sem analisá-los, porque não há como verificar se as informações são precisas e provenientes de uma fonte legítima. O DNS foi criado nos primeiros dias da internet, quando as únicas pessoas ou entidades que se conectavam a ele eram universidades e centros de pesquisa. Não havia razão para esperar que alguém tentasse espalhar informações falsas de DNS.

Apesar desses pontos de grande vulnerabilidade no processo de armazenamento no cache de DNS, não é fácil executar um ataque de envenenamento de DNS. Como o resolvedor de DNS realmente consulta o nameserver autoritativo, os invasores têm apenas alguns milissegundos para enviar uma resposta falsa antes da chegada da resposta real do nameserver autoritativo.

Para executar ataques de falsificação de DNS, os invasores também precisam tentar adivinhar ou ter conhecimento de diversos fatores:

- Quais consultas de DNS não são armazenadas em cache pelo resolvedor de DNS visado, fazendo com que o resolvedor consulte o nameserver autoritativo?
- Qual porta* o resolvedor de DNS está usando: antigamente usava-se a mesma porta para todas as consultas, mas agora utiliza-se uma porta aleatória diferente cada vez que uma consulta é realizada.
- O número de identificação da solicitação
- Para qual nameserver autoritativo a consulta irá

Os invasores também podem obter acesso ao resolvedor de DNS de alguma outra maneira. Se uma pessoa mal-intencionada operar, invadir ou obtiver acesso físico a um resolvedor de DNS, poderá alterar os dados com maior facilidade se estiverem em cache.

*Na rede, uma porta é um ponto virtual de recepção de comunicação. Os computadores possuem várias portas, cada uma com seu próprio número e para que os computadores possam se comunicar entre si, é preciso designar determinadas portas para certos tipos de comunicação. Por exemplo, as comunicações HTTP sempre utilizam a porta 80, enquanto as HTTPS sempre usam a porta 443.

Falsificação e censura de DNS

Vários governos envenenaram intencionalmente os caches de DNS em seus países para negar acesso a determinados sites ou recursos da internet.

Como o DNSSEC poderá ajudar a impedir

Como o DNSSEC poderá ajudar a impedir o envenenamento do DNS?

DNSSEC é uma abreviação de Extensões de Segurança do Sistema de Nomes de Domínio e um meio de verificar a integridade e a origem dos dados de DNS. O DNS foi originalmente projetado sem essa verificação, e por esse motivo o envenenamento do DNS é possível.

Assim como o protocolo TLS/SSL, o DNSSEC usa uma criptografia de chave pública (uma maneira de assinar informações digitalmente) para verificar e autenticar dados. As extensões DNSSEC foram publicadas em 2005, mas o DNSSEC ainda não se tornou lugar-comum, deixando que o DNS continue vulnerável a ataques.

CONTEÚDO RELACIONADO

Nome de domínio

Domain Name Registrar

Segurança de DNS

Registros DNS

DNS reverso

Vendas

Vendas para empresas

Seja um parceiro
Contato de vendas:
+55 (11) 3230 4523

Sobre o DNS

Servidores de DNS

Registros DNS

Glossário de DNS