O que é fluxo rápido de DNS?

Fluxo rápido de DNS é uma forma de trocar rapidamente os endereços de IP associados a um domínio, de modo que os domínios maliciosos utilizados para ataques de phishing e outras atividades criminosas sejam mais difíceis de bloquear.

Protegendo o DNS

Copiar o link do artigo

O que é o fluxo rápido de DNS?

O fluxo rápido de DNS é uma técnica que envolve a associação de vários endereços de IP a um único nome de domínio e a alteração desses endereços de IP rapidamente. Às vezes, centenas ou mesmo milhares de endereços de IP são usados. Os invasores usam o fluxo rápido de DNS para manter suas propriedades da web em funcionamento, ocultar a verdadeira origem de suas atividades maliciosas e impedir que as equipes de segurança bloqueiem seus endereços de IP. Essa técnica é comumente usada por botnets.

Os invasores precisam que seus sites permaneçam ativos para realizar ataques de phishing, hospedar malware, vender informações de cartão de crédito roubadas e realizar outras atividades ilegais. Com o fluxo rápido de DNS, os domínios maliciosos têm mais tempo de atividade e são mais difíceis de bloquear, permitindo que os criminosos cibernéticos realizem mais ataques. Essencialmente, o fluxo rápido do DNS transforma domínios maliciosos em um alvo móvel.

Pense em um assaltante de banco fugindo: se a polícia souber que carro o ladrão está dirigindo, ela pode ficar alerta para o carro com aquela placa e pará-lo antes que saia da cidade. Agora imagine que aquele ladrão de banco tenha um porta-malas cheio de placas e ele sai e troca de placas a cada dois quilômetros. Torna-se muito mais difícil para a polícia identificar o carro do assaltante de banco. O fluxo rápido de DNS tem um efeito semelhante: com o endereço de IP de um site mudando constantemente, é muito mais difícil identificar e bloquear o site.

Como funciona o fluxo rápido de DNS?

Os invasores irão associar vários endereços de IP a um nome de domínio, alterando rapidamente os registros de DNS associados a esse nome de domínio. Um endereço de IP será registrado e, em seguida, cancelado e substituído por um novo endereço de IP a cada poucos minutos ou segundos. Os invasores são capazes de fazer isso explorando uma técnica de balanceamento de carga chamada DNS round robin e definindo um Tempo até entrar no ar (TTL) muito curto para cada endereço de IP. Frequentemente, alguns ou todos os endereços de IP usados serão hosts da web comprometidos pelos invasores. As máquinas nesses endereços de IP atuarão como proxies para o servidor de origem do invasor.

O DNS round robin é uma forma de associar vários servidores da web redundantes, cada um com seu próprio endereço de IP, a um domínio. Quando o nameserver autorizado para esse domínio recebe uma consulta, ele distribui um endereço de IP diferente a cada vez e, como resultado, nenhum servidor web fica sobrecarregado com o tráfego (teoricamente). Embora o balanceamento de carga seja o uso legítimo e intencional do DNS round robin, os invasores podem usar esse recurso para ofuscar suas atividades maliciosas.

Os invasores que usam o fluxo rápido também definirão um TTL muito curto para esses endereços de IP, às vezes até 60 segundos. Assim que o TTL expirar, esse endereço de IP não

estará mais associado a esse nome de domínio.

O que é fluxo rápido duplo?

O fluxo rápido duplo adiciona outra camada de fluxo de DNS, tornando ainda mais difícil bloquear um domínio e rastrear a origem da atividade maliciosa. Com o fluxo rápido duplo, o endereço de IP do nameserver autorizado também é alterado rapidamente. (Uma forma mais técnica de dizer isso é que tanto o registro DNS A para o domínio quanto os registros DNS NS para a zona são alterados constantemente).

Seria como se o assaltante de banco descrito acima não apenas mudasse sua placa continuamente, mas também trocasse de carro continuamente.

Como o fluxo rápido de DNS pode ser evitado?

A maneira mais eficaz de parar o fluxo rápido de DNS é simplesmente retirar o nome do domínio. Por vários motivos, os registradores de nomes de domínio nem sempre estão dispostos ou podem fazer isso.

Os administradores de rede também podem exigir que os usuários de sua rede usem os

servidores DNS que controlam e que bloqueiem ou descartem consultas de domínios maliciosos. Dessa forma, os domínios maliciosos não são resolvidos e os usuários não conseguem acessá-los. Essa técnica é chamada de filtragem de DNS.

CONTEÚDO RELACIONADO

Envenenamento de cache de DNS

DNS sobre TLS

Segurança de DNS

DNS Round-Robin

Registros DNS