Registros DNS, DNSKEY e DS

Os registros DNSKEY e DS são usados pelos resolvedores de DNSSEC para verificar a autenticidade dos registros DNS.

Registros DNS

Copiar o link do artigo

O que são registros DNSKEY e DS?

O Domain Name System (DNS) é a agenda telefônica da internet, mas não foi projetado com a segurança em mente. Por esse motivo, um protocolo de segurança opcional chamado DNSSEC foi criado para que os possuidores de propriedades da web pudessem proteger melhor seus aplicativos. O DNSSEC aumenta a segurança adicionando assinaturas criptográficas aos registros DNS; essas assinaturas podem ser conferidas para verificar se um registro veio do servidor DNS correto.

Para a implementação dessas assinaturas criptográficas, foram criados dois novos tipos de registro DNS: o DNSKEY e o DS. O registro DNSKEY contém uma chave de assinatura pública e o registro DS contém um hash* de um registro DNSKEY.

Cada zona DNSSEC recebe um conjunto de chaves de assinatura de zona (ZSK). Este conjunto inclui uma ZSK privada e pública. A ZSK privada é usada para assinar os registros DNS nessa zona e a ZSK pública é usada para verificar a zona privada.

A ZSK pública é publicada em um registro DNSSEC, que é como ela é fornecida a um resolvedor DNSSEC; o resolvedor usará a ZSK pública para garantir que os registros dessa

zona sejam autênticos. Como uma camada adicional de segurança, as zonas DNSSEC contêm um segundo registro DNSKEY contendo uma chave de assinatura de chave (KSK), que verifica a autenticidade da ZSK pública.

O registro DS é usado para verificar a autenticidade das zonas filhas** das zonas DNSSEC. O registro de chave DS em uma zona pai contém um hash da KSK em uma zona filha. Um resolvedor de DNSSEC pode, portanto, verificar a autenticidade da zona filha fazendo hash de seu registro KSK e comparando-o com o que está no registro DS da zona pai.

**Um hash criptográfico é um embaralhamento unidirecional de entrada alfanumérica; hashes são frequentemente usados para armazenar informações sensíveis como senhas em servidores. Por exemplo, um hash da entrada "cantguessthis" é 18fe9934cf77a759eb2471f2b304708a. Toda vez que "cantguessthis" é colocado na função de hash, ele gera o mesmo hash. Mas não há como obter a entrada original usando apenas o hash. O hash por si só é essencialmente inútil.*

***Uma zona filha é um subdomínio delegado de outra zona. Por exemplo, um URL de example.com pode ter zonas filhas com domínios como blog.example.com e mail.example.com.*