ROOT KSK rollover

2010 keyid 19036

Frederico Neves - NIC.br

GTER 42 - São Paulo - 8/12/2016

A raiz DNS [.] está assinada com extensões de segurança (DNSSEC) desde Jul/2010.

A declaração de práticas operacionais (DPS) DNSSEC da raiz diz que a KSK deve ser trocada sempre que necessário ou após 5 anos de operação.

Esta apresentação explica o processo atualmente em curso pela ICANN (PTI) para efetuar esta troca e porque operadores de rede devem ficar atentos.

Agenda

- DNS e DNSSEC
- Validação
- Rollover
- Trust Anchor Rollover
- Fases
- Cerimônia 27

DNS

- Qual é o endereço IPv6 de d.dns.br ?
  - d.dns.br IN AAAA
- O endereço é 2001:12f8:4::10
  - d.dns.br IN AAAA 2001:12f8:4::10

DNSSEC

- Autenticidade e Integridade via criptografia de chaves publicas.

- Cadeia de confiança das chaves provida pelo registro DS - Como o registro NS para a cadeia de delegações.

- Autenticidade da não existência de um nome ou tipo provida pelo registro NSEC/3. Assinaturas dos intervalos como prova das inexistências. A NSEC D, prova a não existência de B e C.

DNSSEC

- Qual é o endereço IPv6 de d.dns.br c/ DNSSEC ?
  - d.dns.br IN AAAA (*+DO)

- O endereço é 2001:12f8:4::10 + Assinatura
  - d.dns.br IN AAAA 2001:12f8:4::10
  - d.dns.br IN RRSIG AAAA 5 3 172800 (20170209150842 20161201150842 943 dns.br Vo8qg…jN+cby)

Validação

- Processo de inspeção dos dados e assinaturas digitais
  - É necessário uma chave pública, uma cadeia de chaves e um trust anchor
- Validação é mais do que criptografia
  - Resposta é relacionada a pergunta?
  - A resposta está no seu período de validade?
- Por que validar?
  - Proteção dos caches
  - DANE - SMTP Opportunistic TLS encryption
  - Uso agressivo NSEC/NSEC3
    - http://www.iepg.org/2016-11-13-ietf97/Aggressive-NSEC_v0.02.pdf

Rollover

- Boa Prática Criptográfica
  - Segredos não permanecem secretos para sempre
- Boa Prática Operacional
  - Ter um plano completo capaz de ser executado
  - Executar o plano em condições normais
- Por que não um teste privado?
  - Troca da KSK da raiz implica em testar todos que efetuam validação DNSSEC na Internet

Trust Anchor Rollover

- Quanto você não tem um pai… a vida é dura!

  Quando você tem basta incluir/atualizar um DS

- Método manual

  TA em sistemas de controle de versão

  TA embutidas em software

- RFC 5011 - Método automático

  - Melhor forma de atualizar o TA

5011 no Unbound

- Unbound >= 1.4.0 (Nov/2009)

```
server:

  # root key file, automatically updated

  auto-trust-anchor-file: "/usr/local/etc/unbound/root.key"
```

5011 no BIND

- BIND >= 9.8 (Mar/2011)

```
options {

    dnssec-validation auto;

};
```

Possíveis Problemas

- DNS Tamanho das respostas
  - Durante parte do rollover respostas para consultas DNSKEY da raiz podem chegar a 1425 bytes
  - Fragmentação IPv6

http://www.potaroo.net/ispcol/2016-05/v6frags.html

- Não filtrem TCP/53!

Fases

A. Geração - Completada em 27/10/2016 durante cerimônia 27

B. Replicação - Em andamento

   Armazenada fisicamente na KMF Costa Oeste em 28/10/2016

   Importada na HSM na próxima cerimônia - 28 2/2/2017

C. Primeiro SKR contendo a nova chave - Mai/2017

D. Publicação

   11/07/2017

E. Rollover

   11/10/2017

F. Revogação - 11/01/2018

G. Destruição KMF1 - Mai/2018

H. Destruição KMF2 - Ago/2018

Cerimônia 27

- https://www.iana.org/dnssec/ceremony/27
- 27/10/2016 184920 UTC - KMF Costa Leste - Culpeper
- 2017 keyid 20326 - RSA 2048
- SHA256 DS …F8EC8D
- Chave ainda considerada provisória. Aguarda ser importada nas HSMs da KMF Costa Oeste - Los Angeles durante a cerimônia 28 em 2/2/2017

Referências

- https://www.icann.org/kskroll
- https://www.iana.org/dnssec
- https://tools.ietf.org/html/rfc5011
- https://tools.ietf.org/html/rfc6781
- https://www.unbound.net/documentation/howto_anchor.html
- http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch06.html#managed-keys

Perguntas?

Obrigado!