# Colisões em DNS

Rubens Kühl

(GTER-36 São Paulo, 12/2013)

# Não deveriam acontecer, mas...

# Definição e Origens

- Definição: quando a resposta DNS não é a resposta esperada em função de alterações não maliciosas realizadas fora da rede da organização

- Possíveis origens:

  - Uso interno de nomes que não eram delegados em algum nível da hierarquia DNS

  - Uso de *search lists*

  - Uso (desrecomendado) de raízes alternativas

# Por que agora ?

- Evidenciada pelo programa de novos gTLDs

- Exacerbada em função de interesses comerciais e preocupações com *liability*

- Oportunidade para identificar e mitigar riscos reais

# O que vem por aí

- Alguns novos gTLDs já delegados (http://newgtlds.icann.org)
  - شبكة., .みんな
  - .guru, .uno
- Outros a caminho
  - .bom, .final, (…1300+…)

# Nomes DNS Internos

- Imaginados para aplicações restritas à rede interna de uma organização.
- www.corp,  www.contabil,  mail.test
- Não terminam em um TLD válido, mas não há, ainda, equivalentes DNS da RFC 1918 (nem mesmo as RFC 6761-2)
  - Delegação gera possíveis colisões
- Colisões também pode acontecer com 2LDs/3LDs não registrados

# DNS-SD/Bonjour-based namespaces"

- 63 different namespaces are making DNS-SD queries!

| Example Namespaces |
|---|
| "U"$OKI$/>"6"3@PU"% |
| "I@I3&@PU"% |
| "I.I3(@PU"% |
| "I."X"$/)@PU"% |
| "I."X"$/9@PU"% |
| U@$"LK$"8@PU"% |
| U@2./8@".@8KP"8@PU"% |
| /2PIKA<@-$K@PU"% |
| /.PIX"->-$@"X<>"6-@PU"% |
| NI$I:@PU"% |
| N#I2K$$K<I)@PU"% |

- Stelmat is a networking company based in Cuiaba, Brazil (0.5% of CBA queries)!


- Makuhari Baytown High-rise in Chiba, Japan (4.9% of

# Também afetará redes daqui

# *Search Lists*

- Serviriam para ajudar usuários mapeando automaticamente nomes incompletos em FQDNs (*Fully Qualified Domain Names)*
  - Exemplo: www -> www.exemplo.com.br -> Endereço IP
- Porém, a RFC 1535 diz que nomes que contenham “.” devem ser primeiro tentados na raiz
  - Exemplo: www.uno -> www.uno -> NXDOMAIN -> www.uno.exemplo.com.br -> Endereço IP

# Mitigação nos novos gTLDs

- Bloqueio por alguns meses de consultas DNS já observadas na raiz nos últimos 8 anos

- Desenvolvimento de um plano de mitigação individualizado para cada *string*

- Possibilidade de pedir desativação de um domínio que gere impacto ruim demonstrável

# Prevenção

- Utilização de FQDNs mesmo se houverem *search lists*
- Desativação de *search lists*
- Migração de nomes DNS internos para *views* internas como interno.exemplo.com.br
- Delegação temporária em servidor interno