DNS - Por que DNSSEC agora mais do que nunca ?

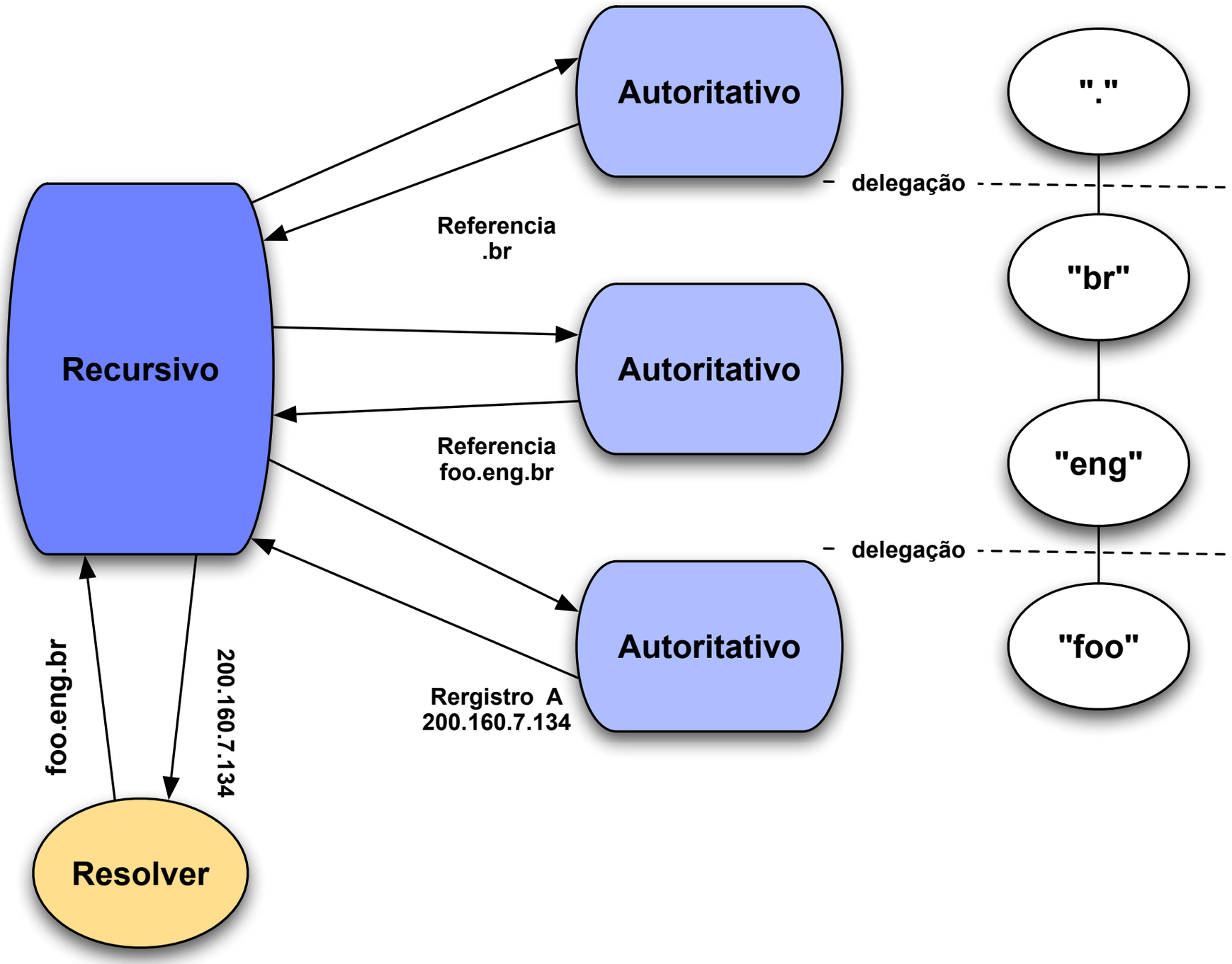
Frederico Neves <fneves@registro.br>

GTS12 - São Paulo - 20081108

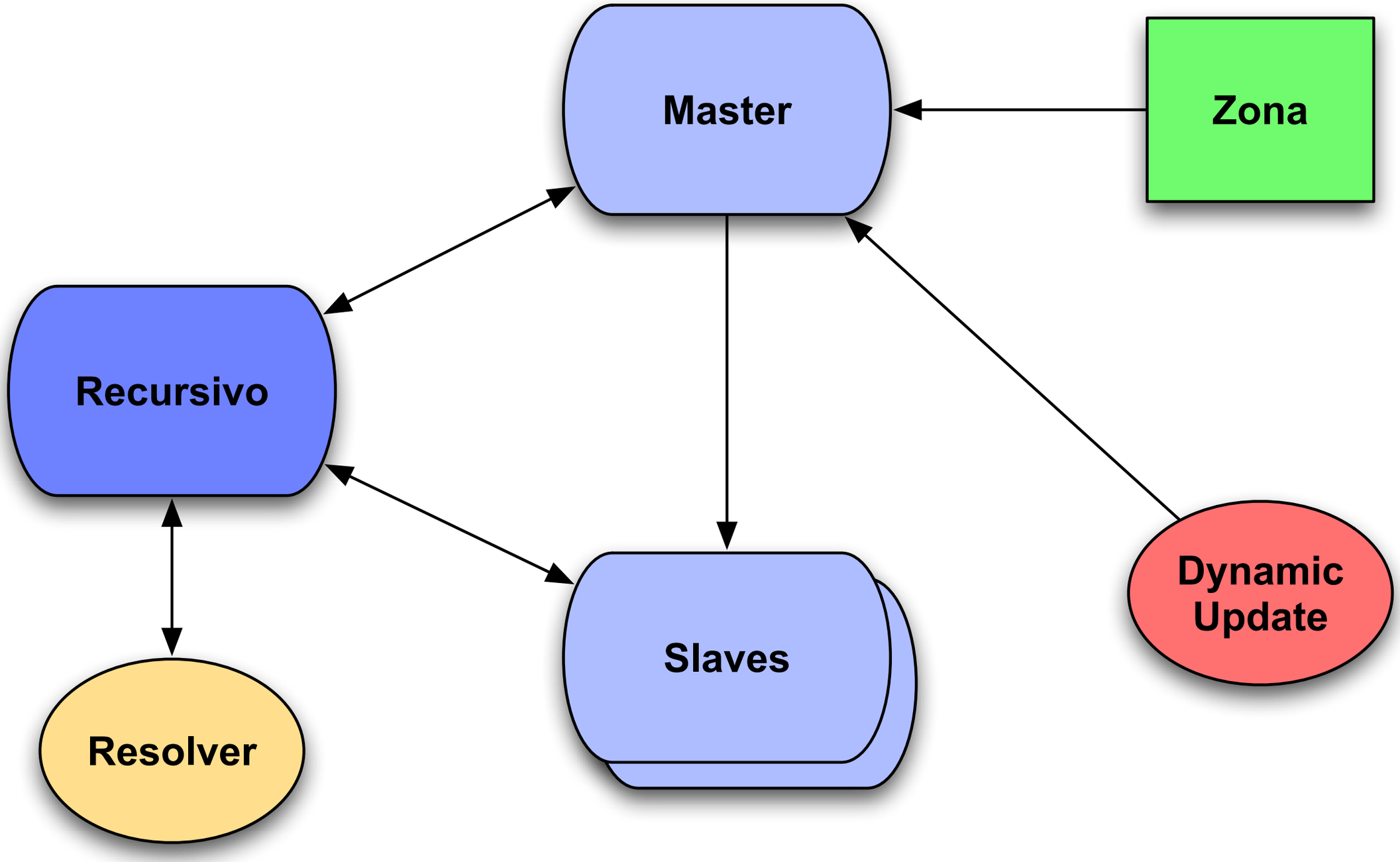
DNS

- Foi criada originalmente em 1984 em substituição ao HOSTS.TXT.
- Utilizou tecnicas de bases de dados distribuidas desenvolvidas nas décadas anteriores.
- É a maior base de dados distribuida existente
- É extremamente escalavel. Somente os sevidores para o .br respondem 3 bilhões de consultas por dia.
- Sofreu várias alterações no standard durante estes 25 anos sem perda da compatibilidade para a resolução de problemas administrativos, de implementações, segurança, etc...
- Praticamente tudo quando se fala em **Internet** depende de DNS

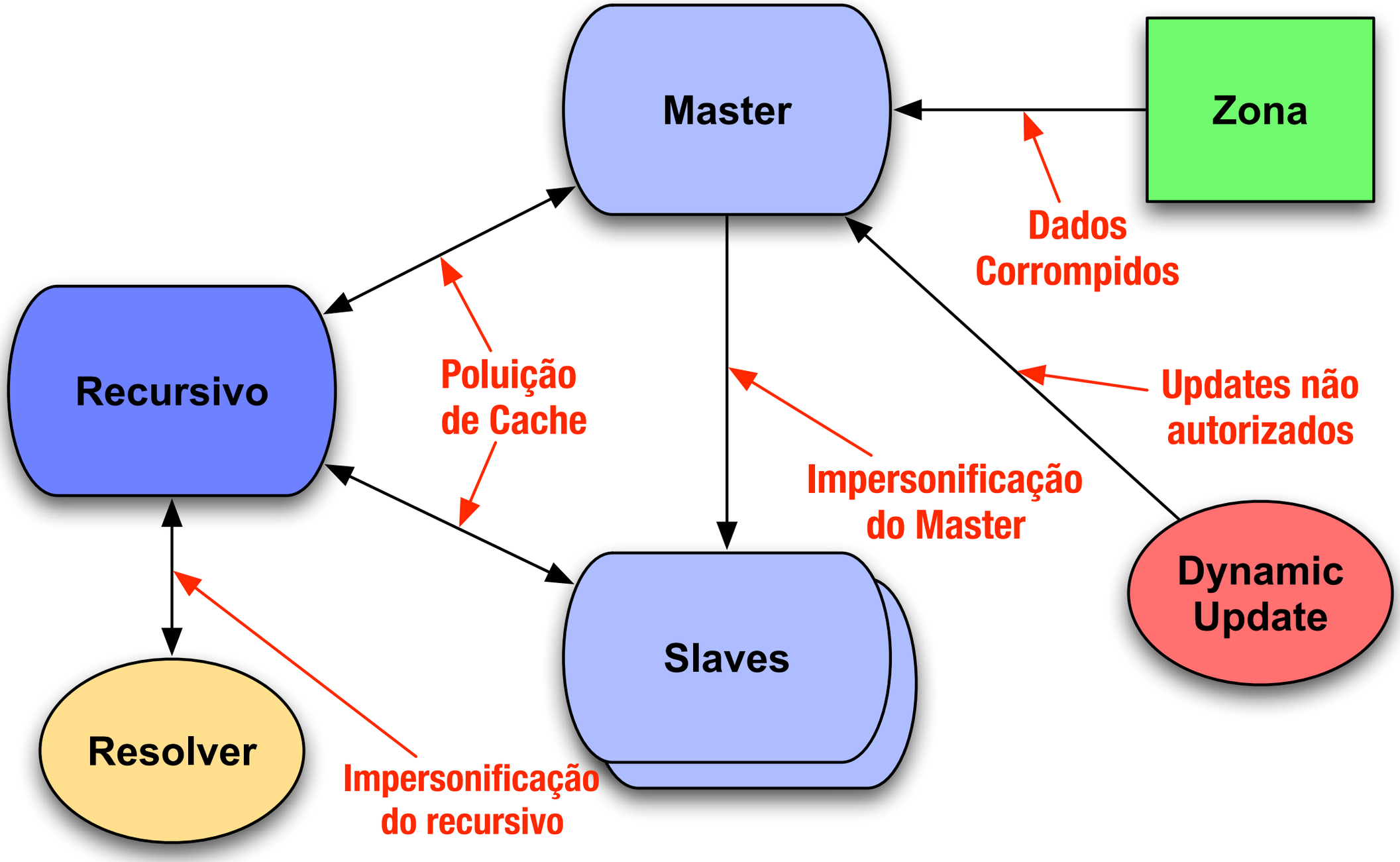
Exemplo de resolução DNS



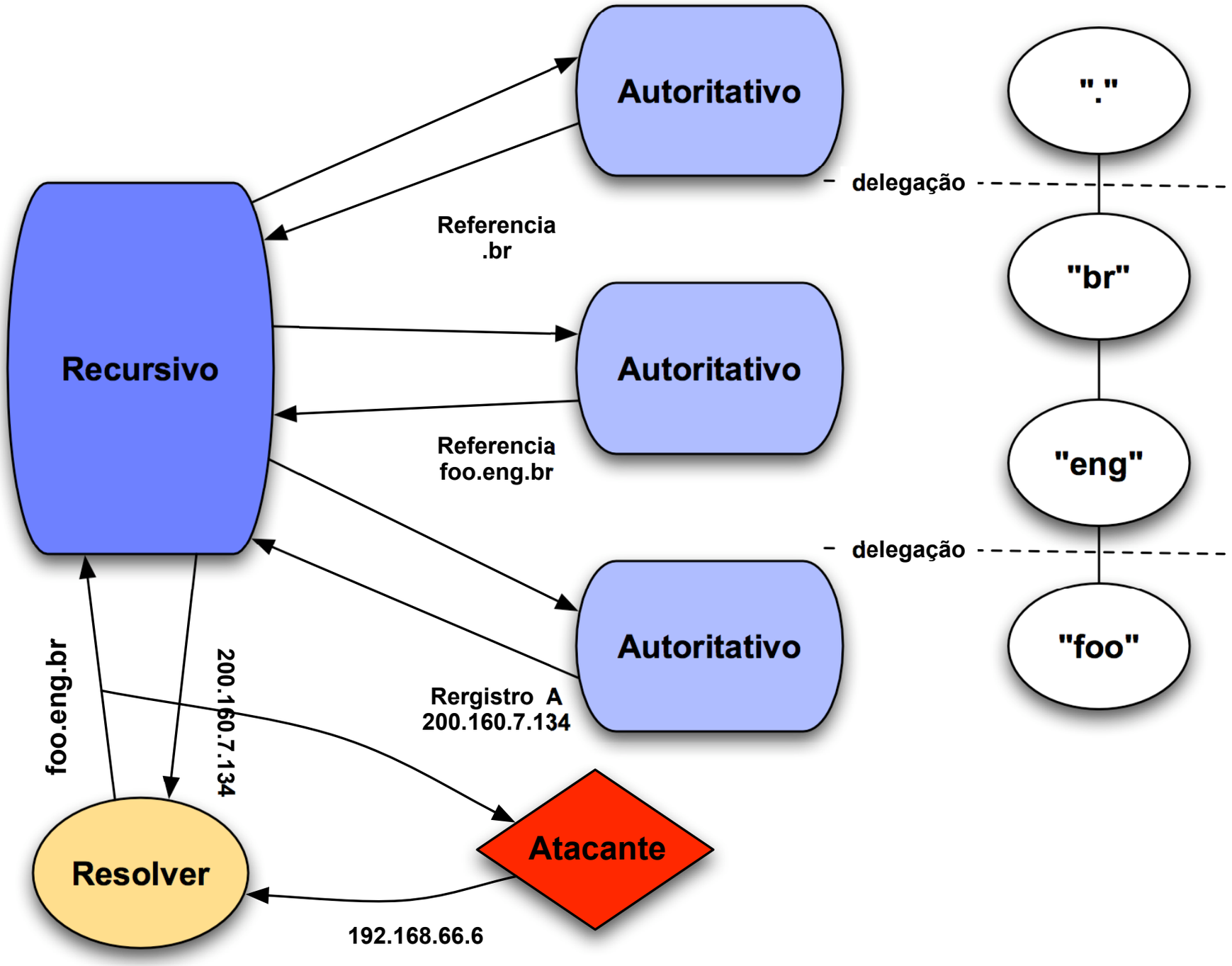
DNS - Fluxo de Informação



DNS - Vulnerabilidades



Exemplo de ataque “on-path”



Ataque DNS - Kaminsky style

- Tradicional poluição de cache via pacote UDP forjado com a adição de “glue records” - Por que a BCP38 é tão difícil de implementar ???

- Inovação pelo uso de sub-domínios da vítima subvertendo o cache negativo e assim tornando praticamente ilimitado o número de tentativas do ataque

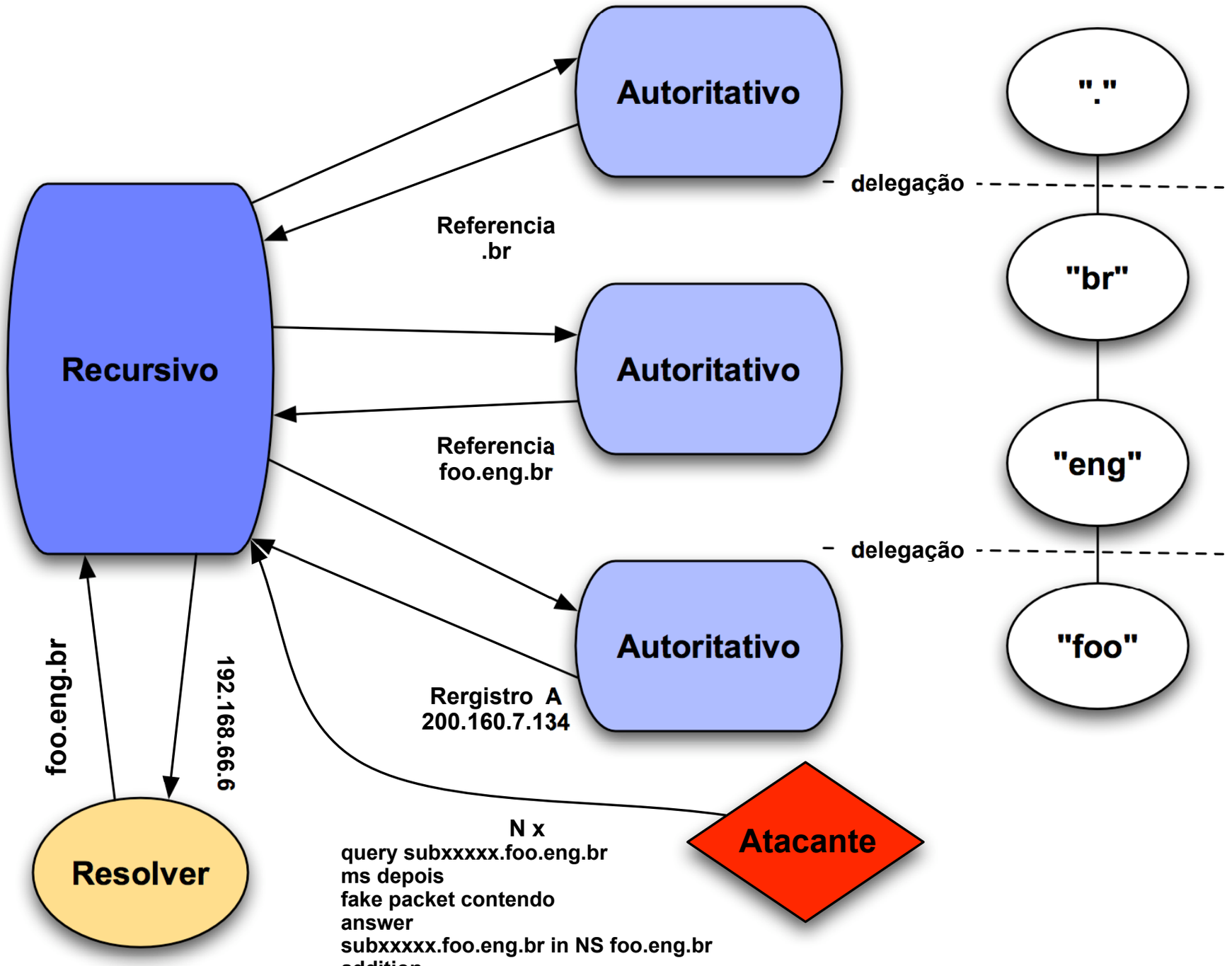
- Abuso do “ranking” de dados para entrada no cache via seção adicional (rfc2181 5.4.1)

- Birthday attack

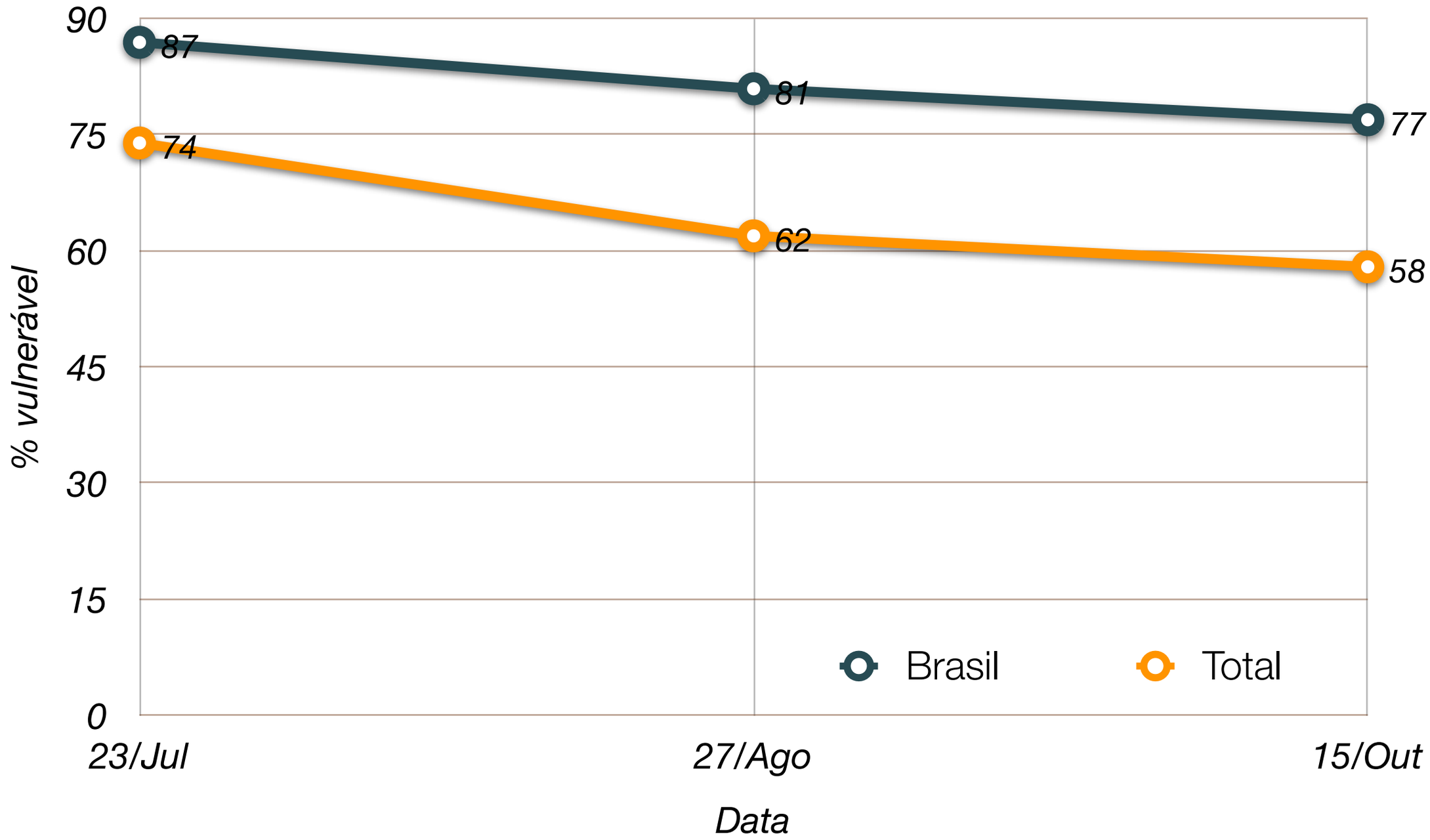
- Servidores sem mitigação via randomização de portas podem ser efetivamente subvertidos em ataques cegos em menos de 5 segundos.

  p 0.5 - sem patch 16bits ~320 pkts, patched ~31bits ~58k pkts !

Exemplo de ataque “blind”



Servidores Vulneráveis



RFC2181 - Efeito Colateral

- Interpretação mais estrita da seção 5.4.1 (data ranking)

  Ainda em processo de padronização

  http://www.ietf.org/internet-drafts/draft-ietf-dnsext-forgery-resilience-07.txt

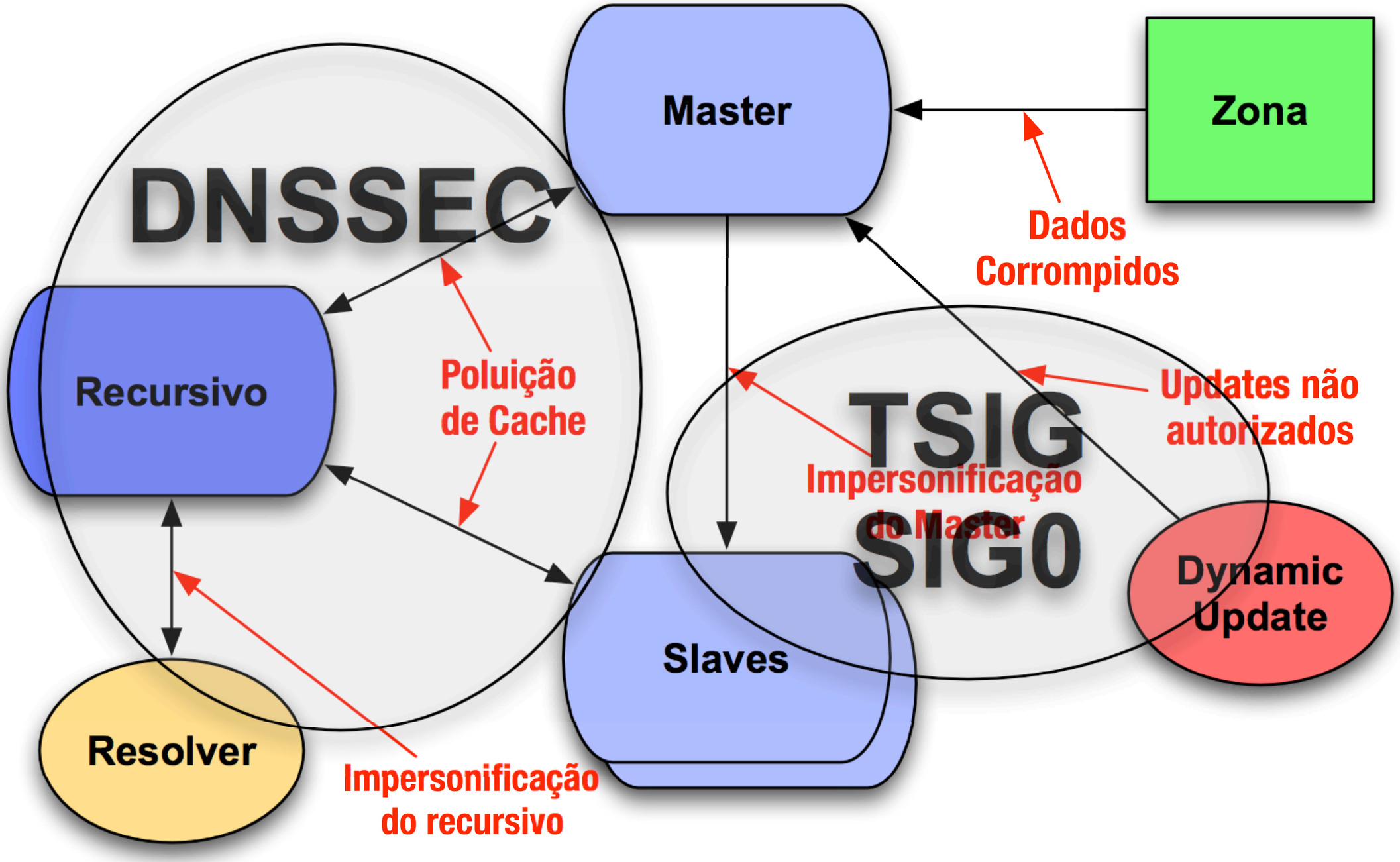
- Própria 2181 limita TTL dentro de um RRset (5.2)

- **Atenção**

  Caso servidores residam dentro da mesma zona, e sejam necessários glue records no seu parent, os TTLs dos RRsets dos seguintes tipos devem ser iguais.

  NS - A - AAAA

Soluções disponíveis



DNSSEC em um slide

- Autenticidade e Integridade são providas pela assinatura dos RRsets com uma chave privada
- Zonas delegadas assinam seus RRsets com a sua chave privada
  - Autenticidade da chave é verificada pela assinatura na zona pai do registro DS (hash da chave pública da zona filha)
- Chave pública é usada para verificar RRSIGs dos RRsets
- Autenticidade da não existência de um nome ou tipo é provida por uma cadeia de registros que aponta para o próximo nome em uma sequência canônica (NSEC)

Disponibilidade

- Início em 4/6/2007

  br

  blog.br

  eng.br

  eti.br

  gov.br

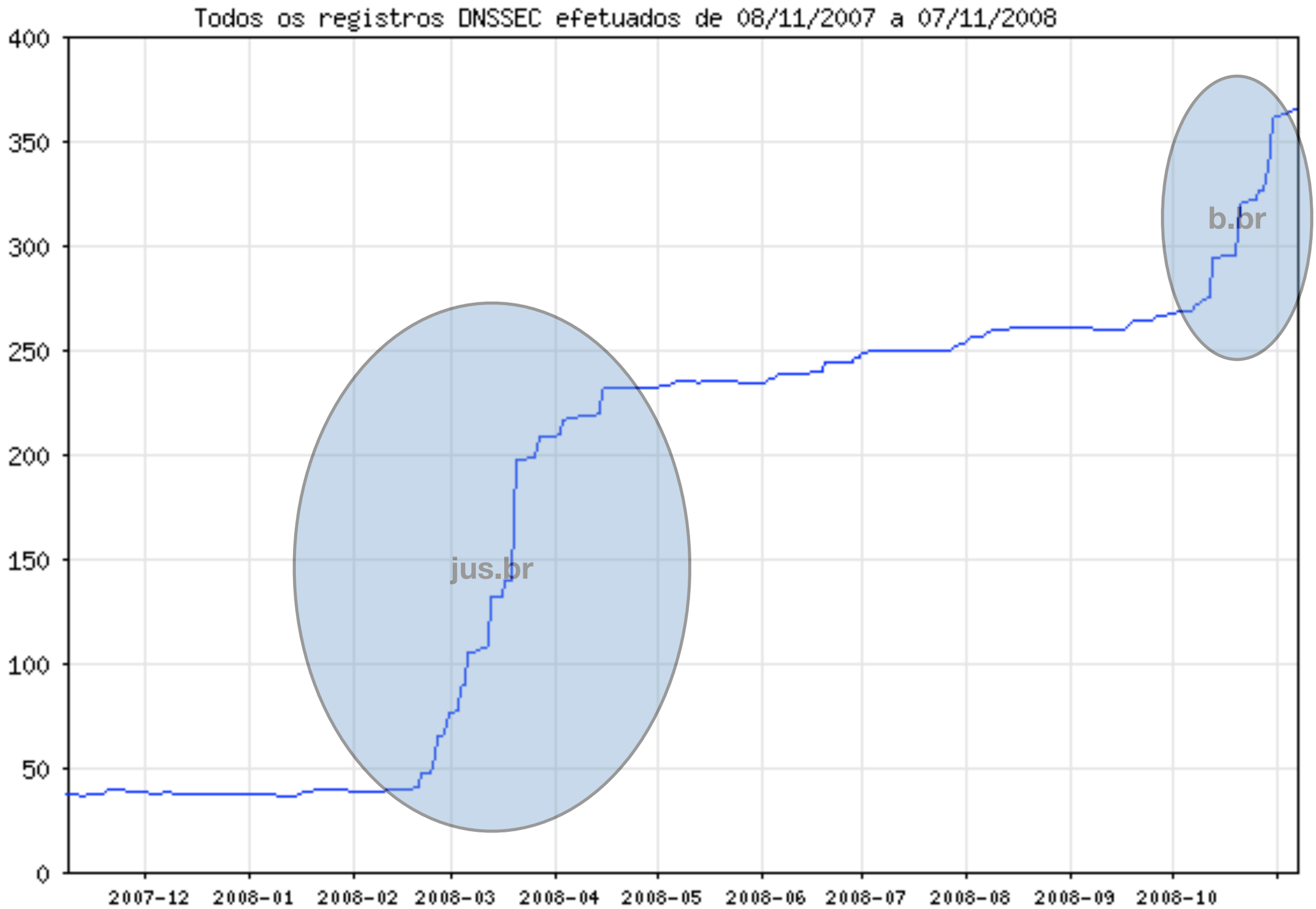
- Disponível atualmente em quase todos os domínios de segundo-nível

  http://registro.br/info/dpn.html

- Farta documentação disponível com referências no FAQ do Registro.br

  http://registro.br/faq/faq8.html#23

Crescimento



Disponibilidade de Software

- Bind 9.5.0 (recursivo e autoritativo)

  http://www.isc.org/index.pl?/sw/bind/index.php

- NSD 3.1.1 (autoritativo)

  http://www.nlnetlabs.nl/nsd/index.html

- Unbound 1.0.2 (recursivo com suporte para nsec3)

  http://unbound.net/

Próximos passos

- .com.br e .org.br

  Maiores zonas representando 95% de todos os domínios abaixo do .br

  DS opcional

- Quando

  Tão logo tenhamos servidores autoritativos BIND e NSD estáveis com suporte a RFC 5155

  BIND 9.6 planejado para o início de 2009.

- Teste já em produção com o domínio sec3.br

  http://registro.br/faq/faq8.html#24

Perguntas ?

Obrigado !