Introdução a DNS & DNSSEC [1]

David Robert Camargo de Campos
Rafael Dantas Justo
<tutorial-dnssec@registro.br>

Registro.br

[1] versão 1.5.0 (Revision)
A última versão deste tutorial pode ser encontrada em: ftp://ftp.registro.br/pub/doc/introducao-dns-dnssec.pdf

DNS - Domain Name System

O Sistema de Nomes de Domínio é um banco de dados distribuído. Isso permite um controle local dos segmentos do banco de dados global, embora os dados em cada segmento estejam disponíveis em toda a rede através de um esquema cliente-servidor.

- Arquitetura hierárquica
- Distribuída eficientemente, sistema descentralizado e com cache
- O principal propósito é a resolução de nomes de domínio em endereços IP e vice-versa

exemplo.foo.eng.br	$\longleftrightarrow$	200.160.10.251
www.cgi.br	$\longleftrightarrow$	200.160.4.2
www.registro.br	$\longleftrightarrow$	2001:12ff:0:2::3

Registro de domínios (.br)

- Reserva o direito da pessoa física ou jurídica sobre um determinado nome de endereço na Internet.
- Domínios não registrados não podem ser encontrados na Internet.

Sistema WEB

A interface WEB permite de maneira prática gerenciar os domínios de qualquer pessoa física ou jurídica.

– http://registro.br/ajuda/registro-de-novos-dominios/

Publicação quasi-on-line

registro.br
Registro de Domínios para a Internet no Brasil

O que é uma Publicação?

As modificações que são realizadas pela interface de provisionamento não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS a qual atualiza o sistema DNS.

nic.br

Publicação quasi-on-line

registro.br
Registro de Domínios para a Internet no Brasil

O que é uma Publicação?

As modificações que são realizadas pela interface de provisionamento não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS a qual atualiza o sistema DNS.

As publicações DNS ocorrem a cada 30 minutos

- No caso do registro de um novo domínio ele já estará visível na Internet após a próxima publicação.
- No caso da alteração de dados de um domínio, após a próxima publicação, o domínio passará por um período de transição que poderá durar até 24 horas.

nic.br

Tipos de servidores

registro.br
Registro de Domínios para a Internet no Brasil

Servidor Autoritativo

Ao receber requisições de resolução de nome, responde um endereço caso possua, uma referência caso conheça o caminho da resolução ou uma negação caso não conheça

Servidor Recursivo

Ao receber requisições de resolução de nomes, faz requisições para os **servidores autoritativos** e conforme a resposta recebida dos mesmos continua a realizar requisições para outros **servidores autoritativos** até obter a resposta satisfatória

nic.br

Tipos de dados que podem ser armazenados

Os dados associados com os nomes de domínio estão contidos em **Resource Records** ou **RR**s (Registro de Recursos)

- Atualmente existe uma grande variedade de tipos

Alguns Tipos Comuns de Records

SOA	Indica onde começa a *autoridade* a zona
NS	Indica um *servidor de nomes* para a zona
A	Mapeamento de nome a endereço (IPv4)
AAAA	Mapeamento de nome a endereço (IPv6)
MX	Indica um *mail exchanger* para um nome (servidor de email)
CNAME	Mapeia um nome alternativo (apelido ou indireção)
TXT	Campo de texto livre

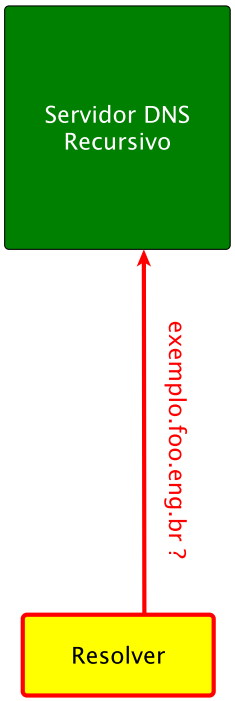
Exemplo de requisição de endereço

Resolver

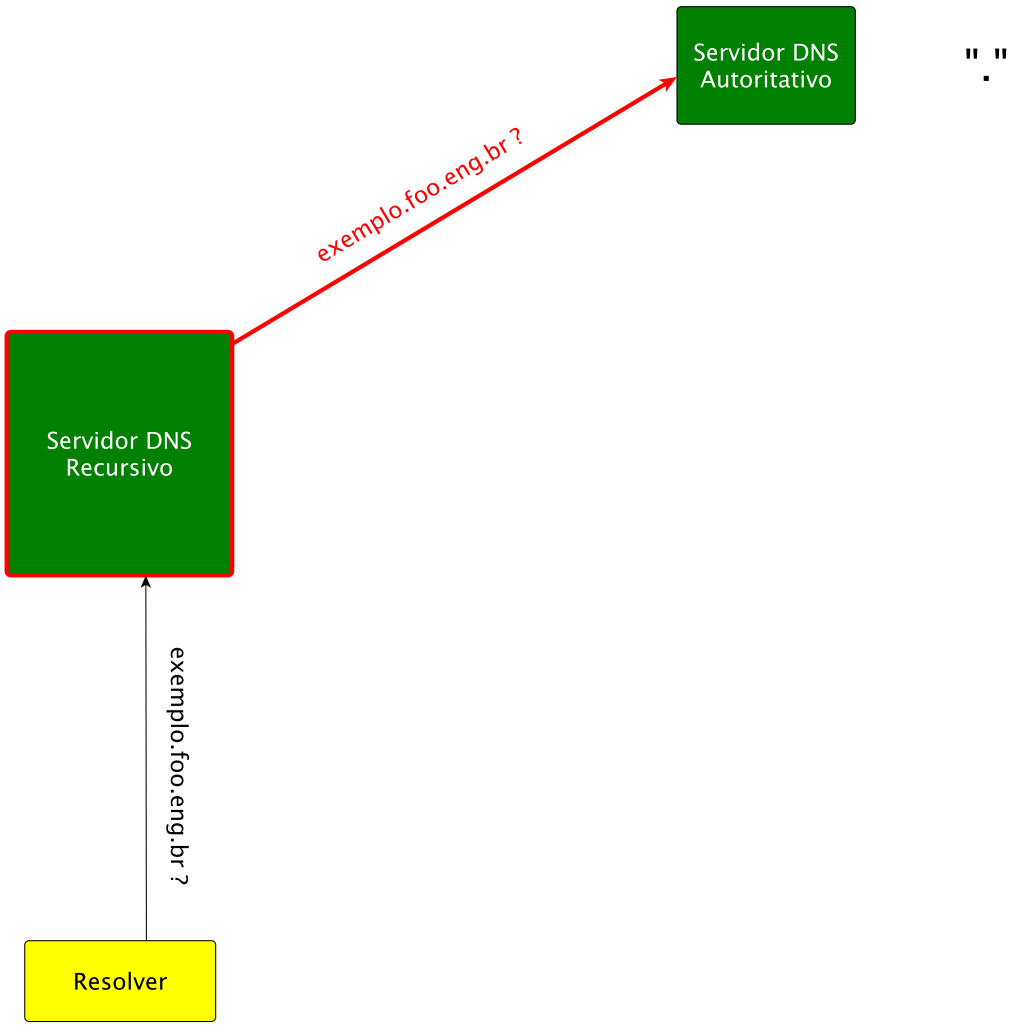
Serviço localizado no cliente que tem como responsabilidade resolver as requisições DNS para diversos aplicativos

Exemplo de requisição de endereço

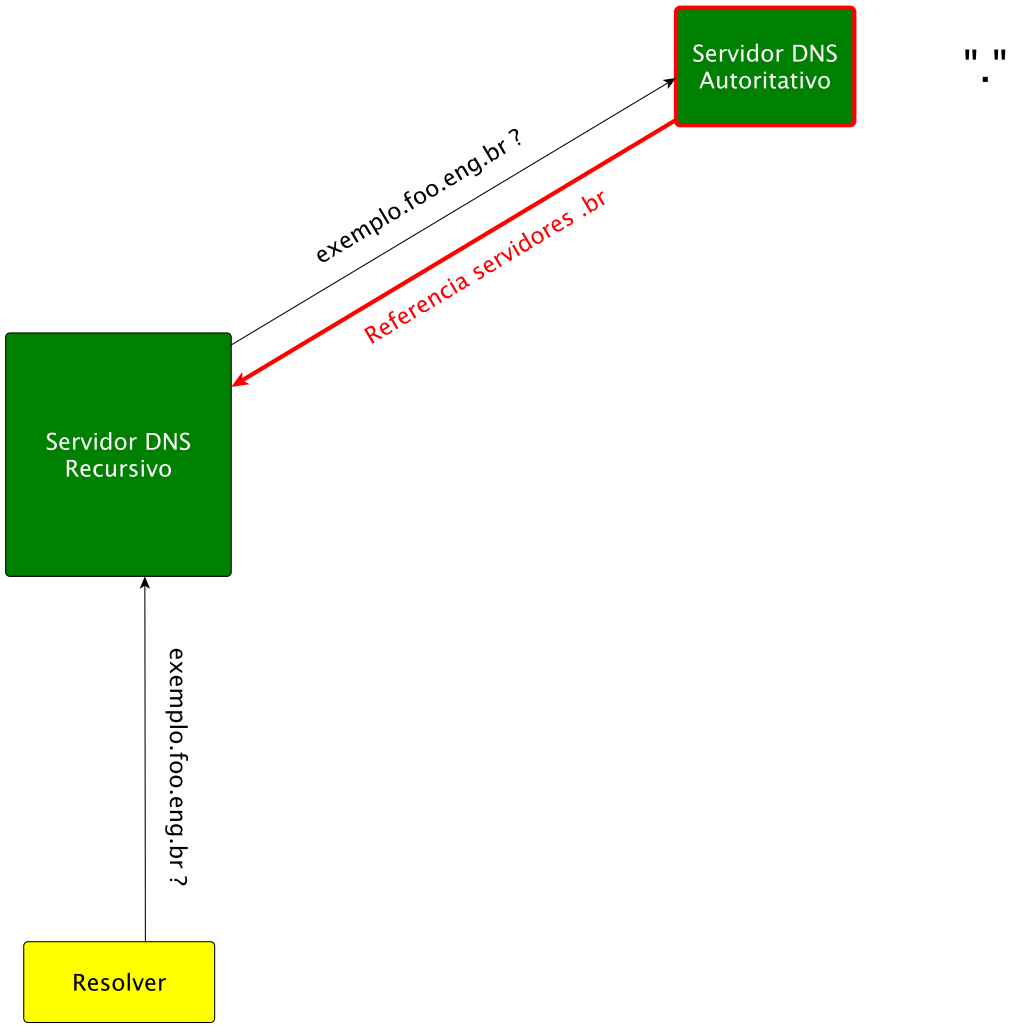
Supondo que o *cache* está vazio ou sem informações relevantes



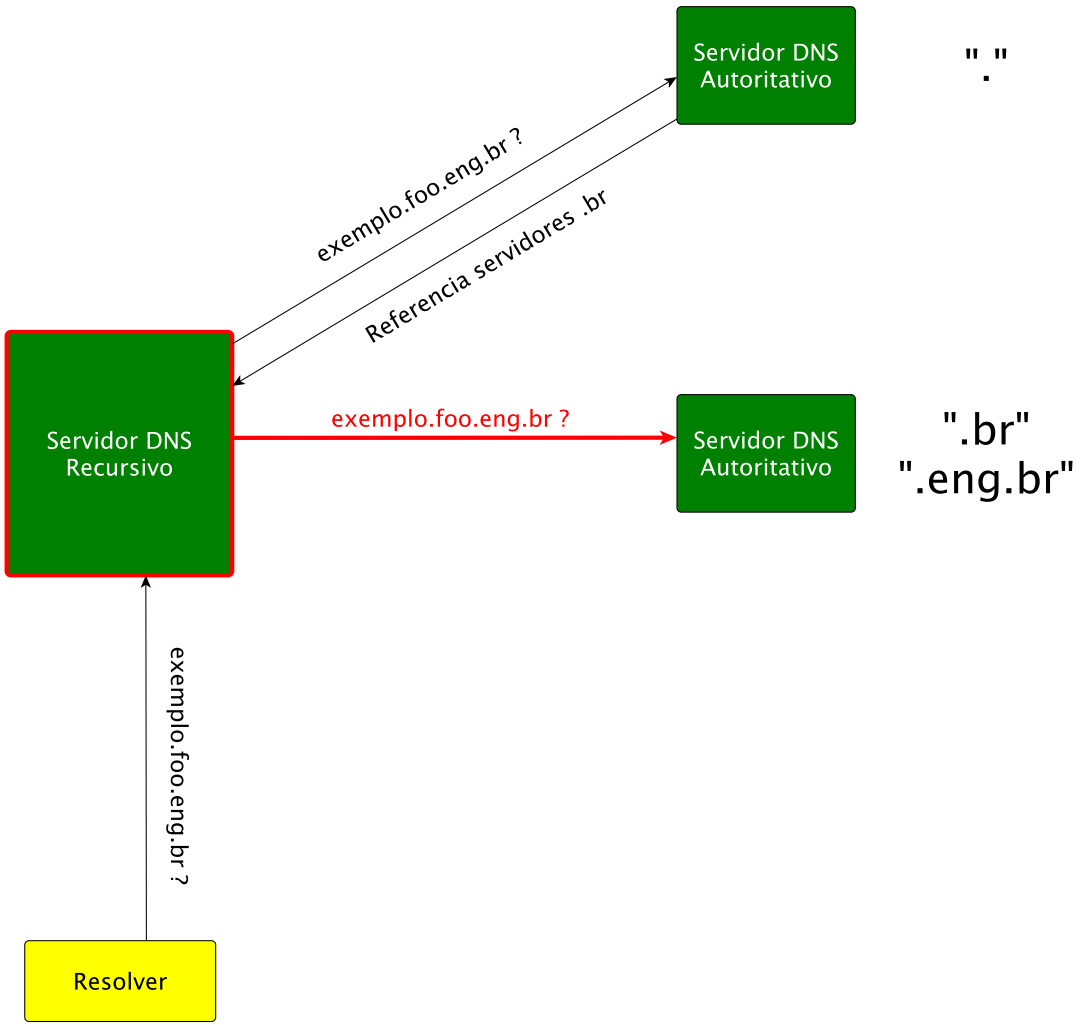
Exemplo de requisição de endereço



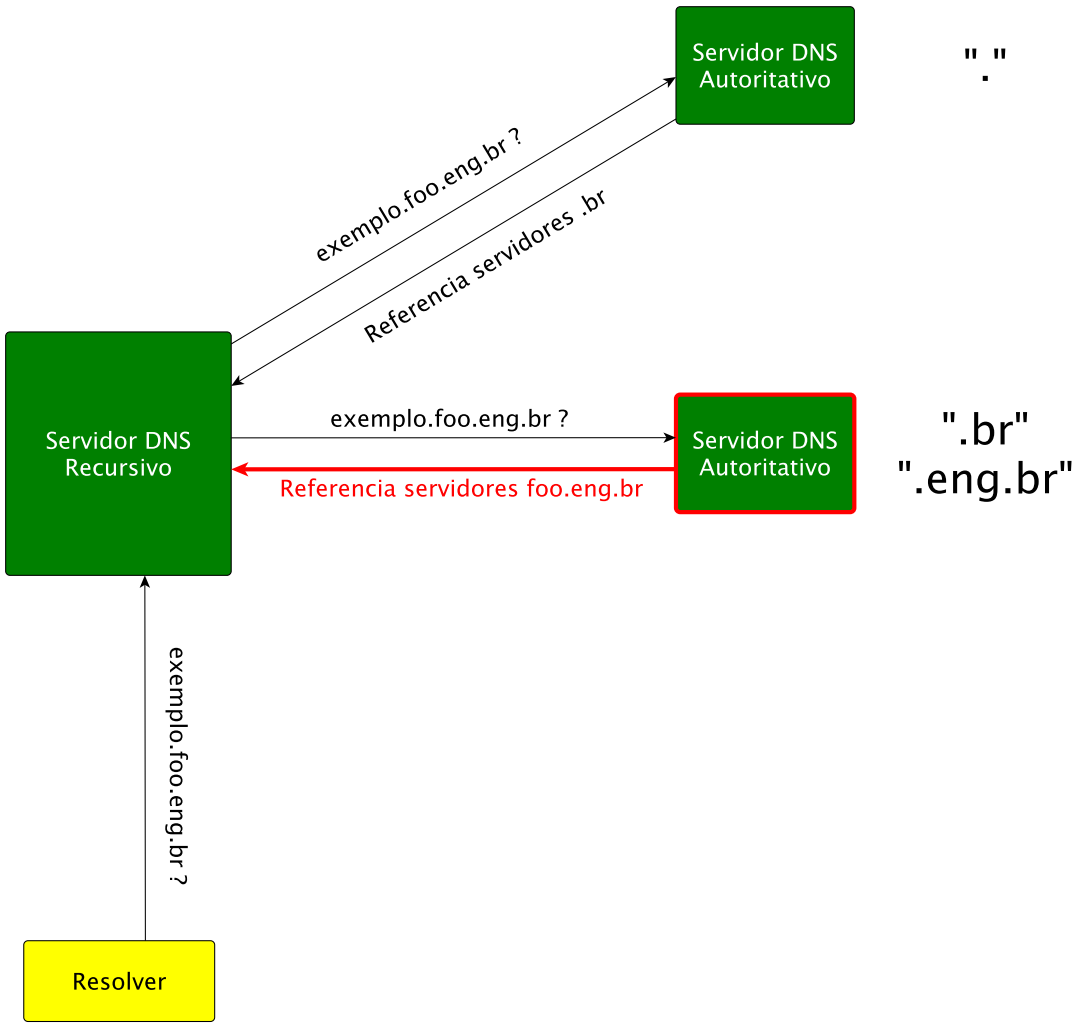
Exemplo de requisição de endereço



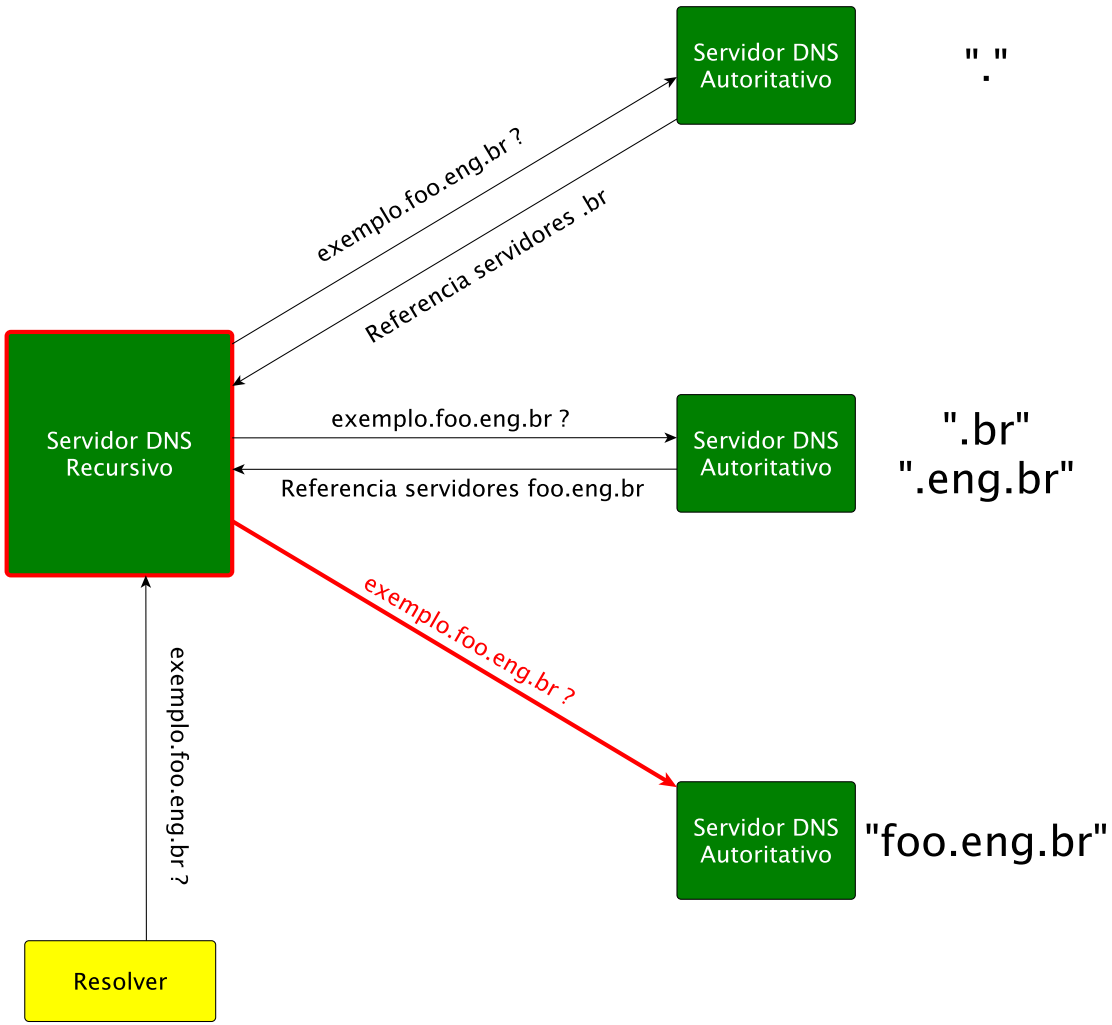
Exemplo de requisição de endereço



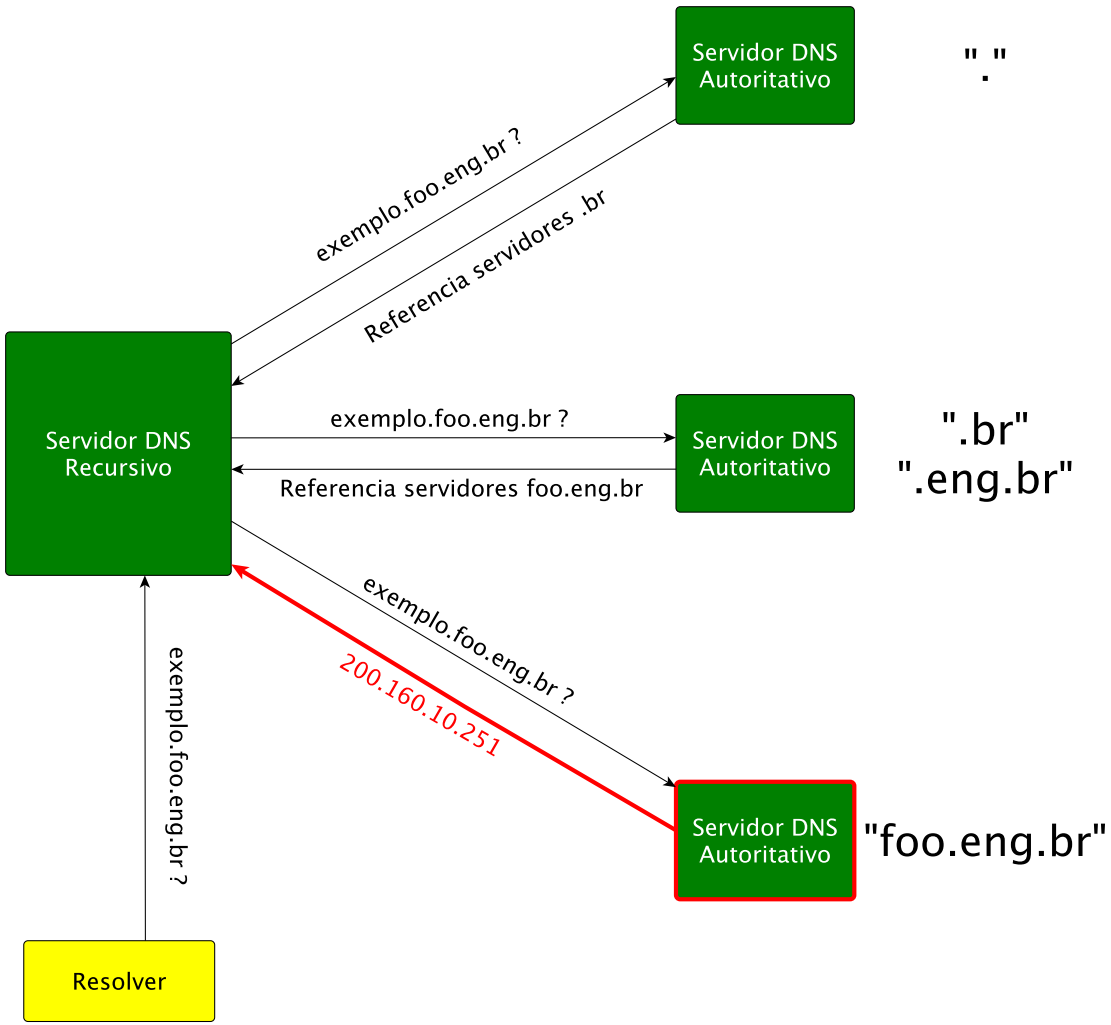
Exemplo de requisição de endereço



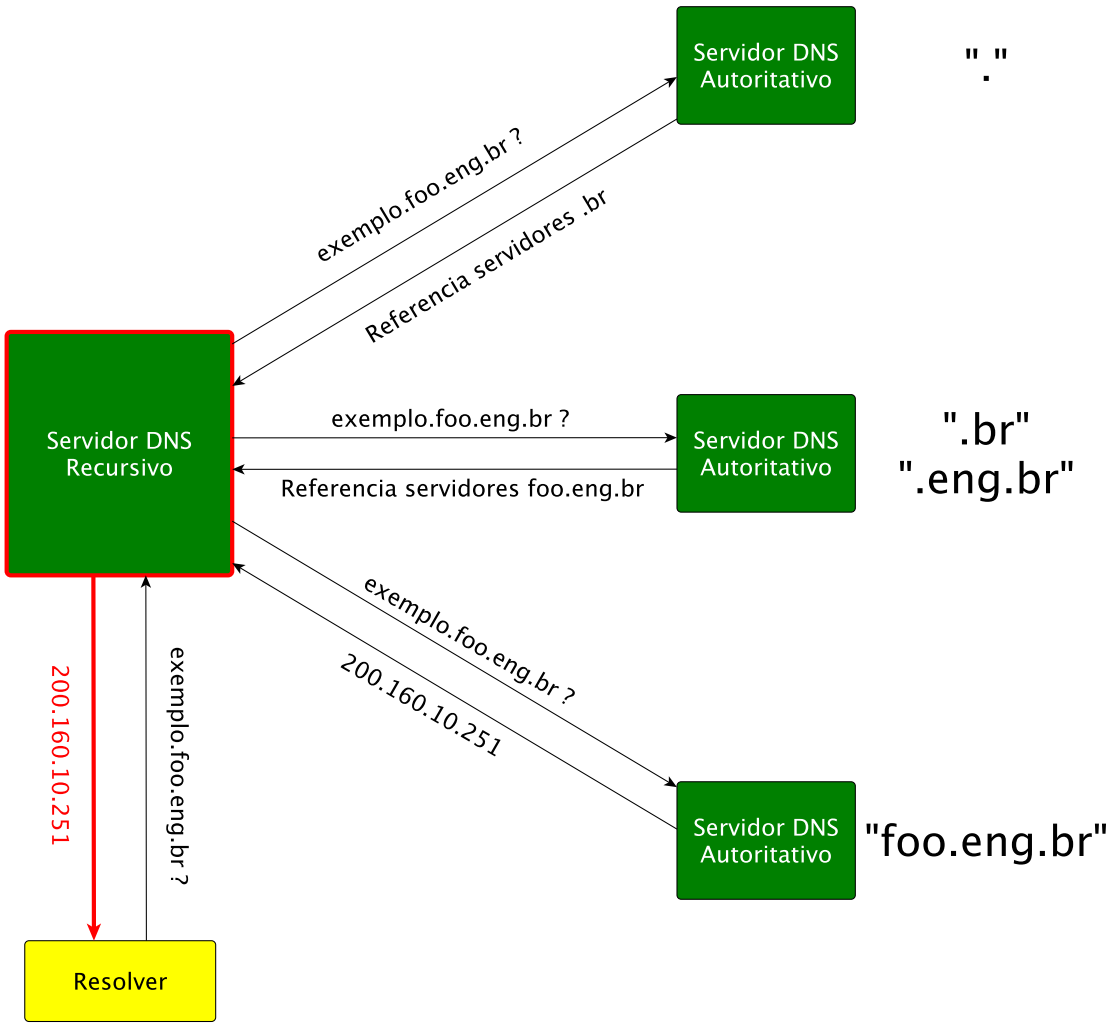
Exemplo de requisição de endereço



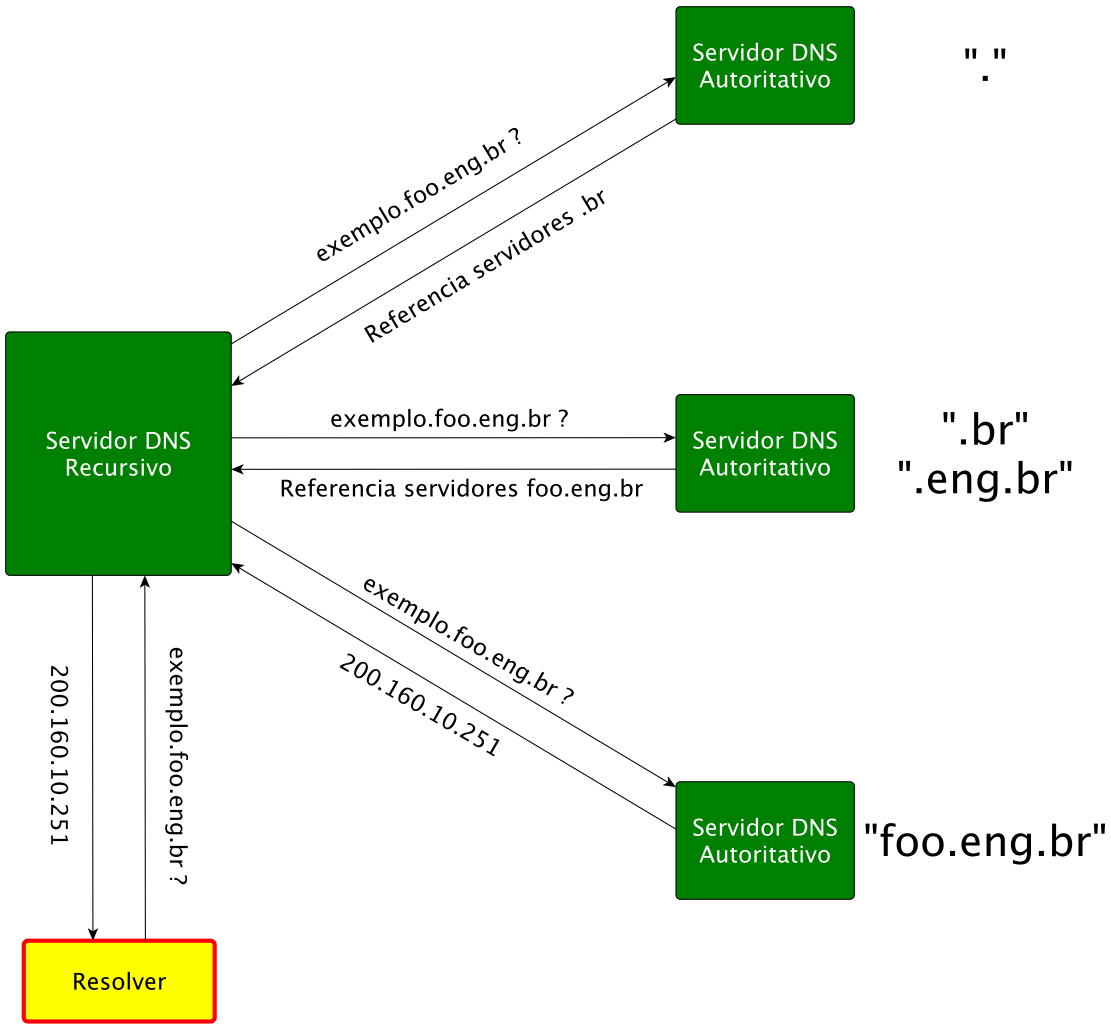
Exemplo de requisição de endereço



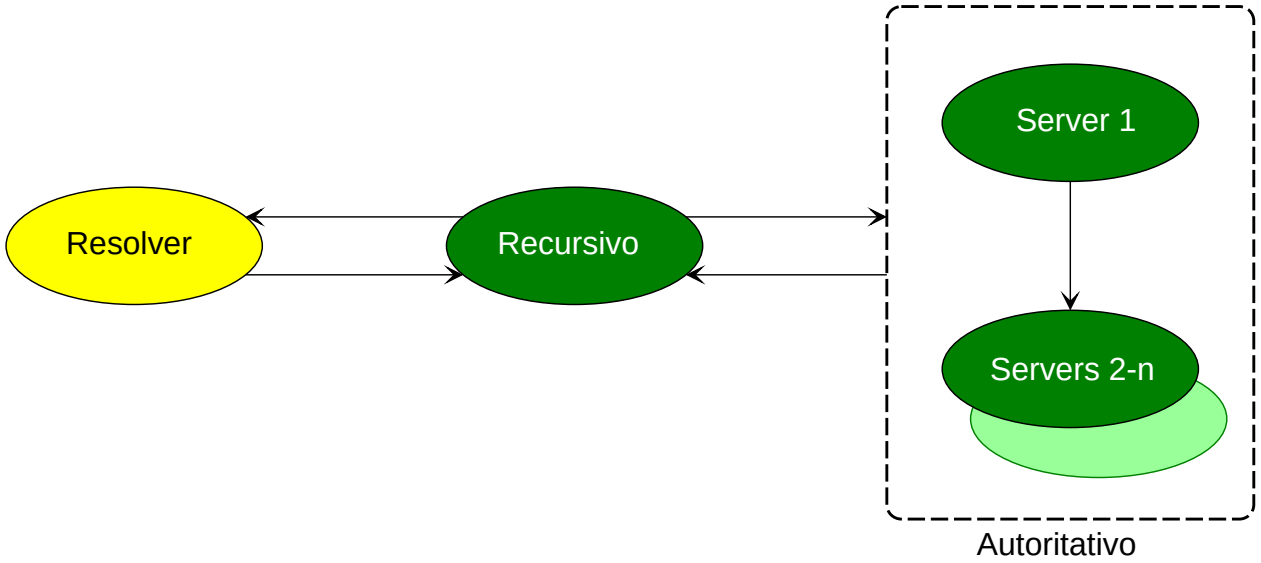
Exemplo de requisição de endereço



Exemplo de requisição de endereço

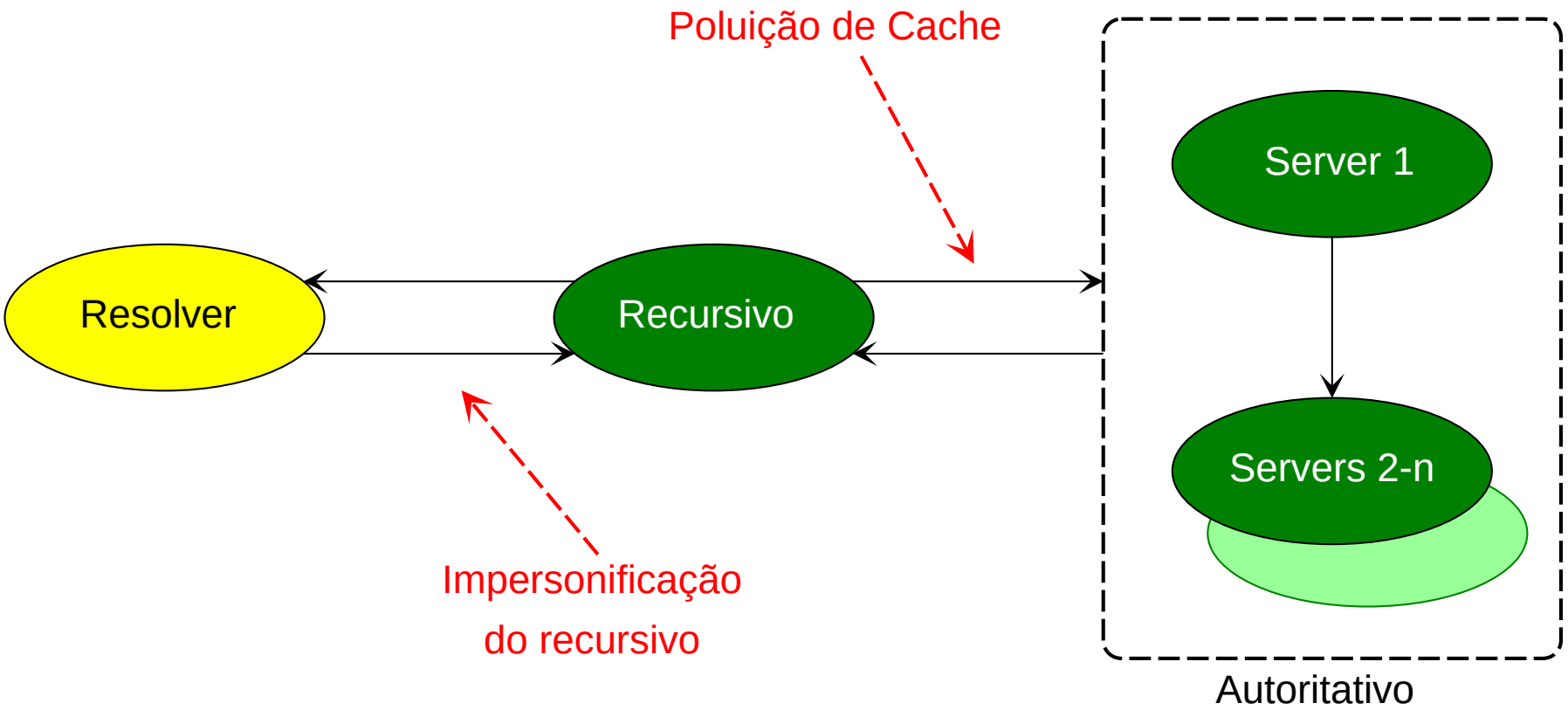


Fluxo de dados



1. Resolver faz consultas no Recursivo
2. Recursivo faz consultas no Autoritativo (Servidor 1 ou Servidor[2-n])
3. Servidor 1 tem os dados originais
4. Servidor[2-n] recebe os dados do Servidor 1

Vulnerabilidades

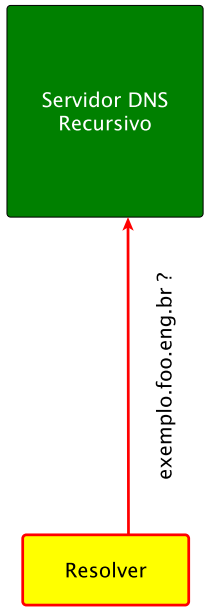


Exemplo de Ataque

Poluição de Cache

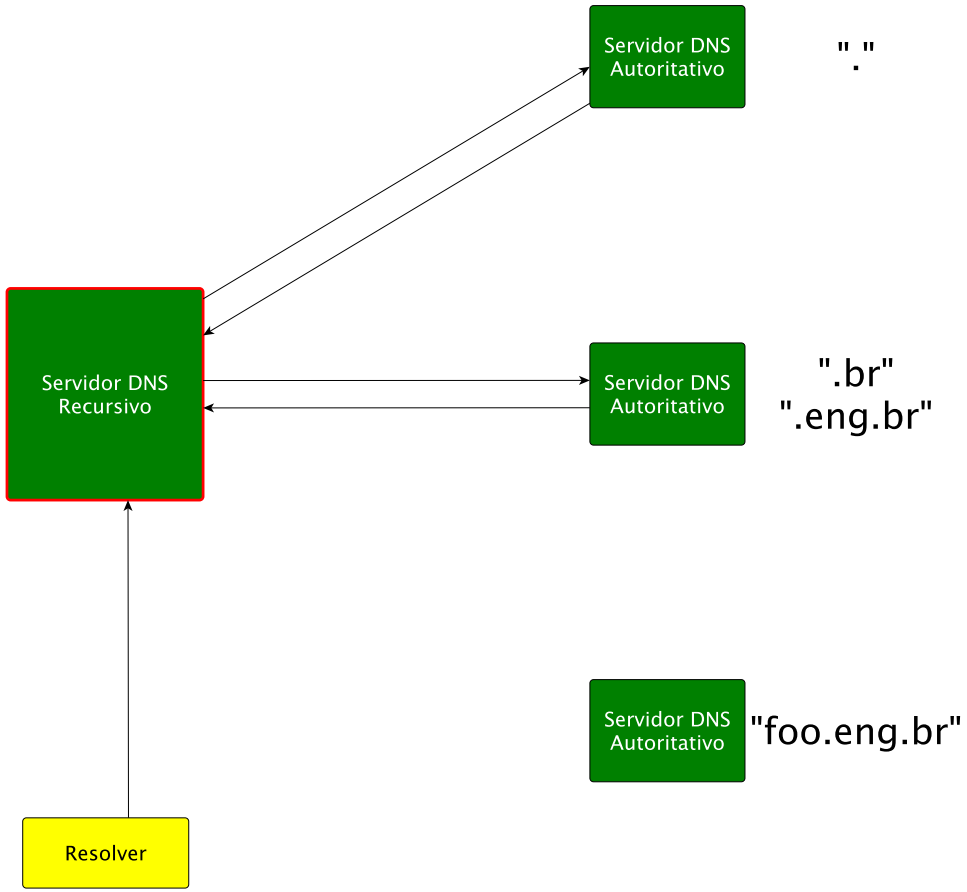
Exemplo de Ataque

Poluição de Cache



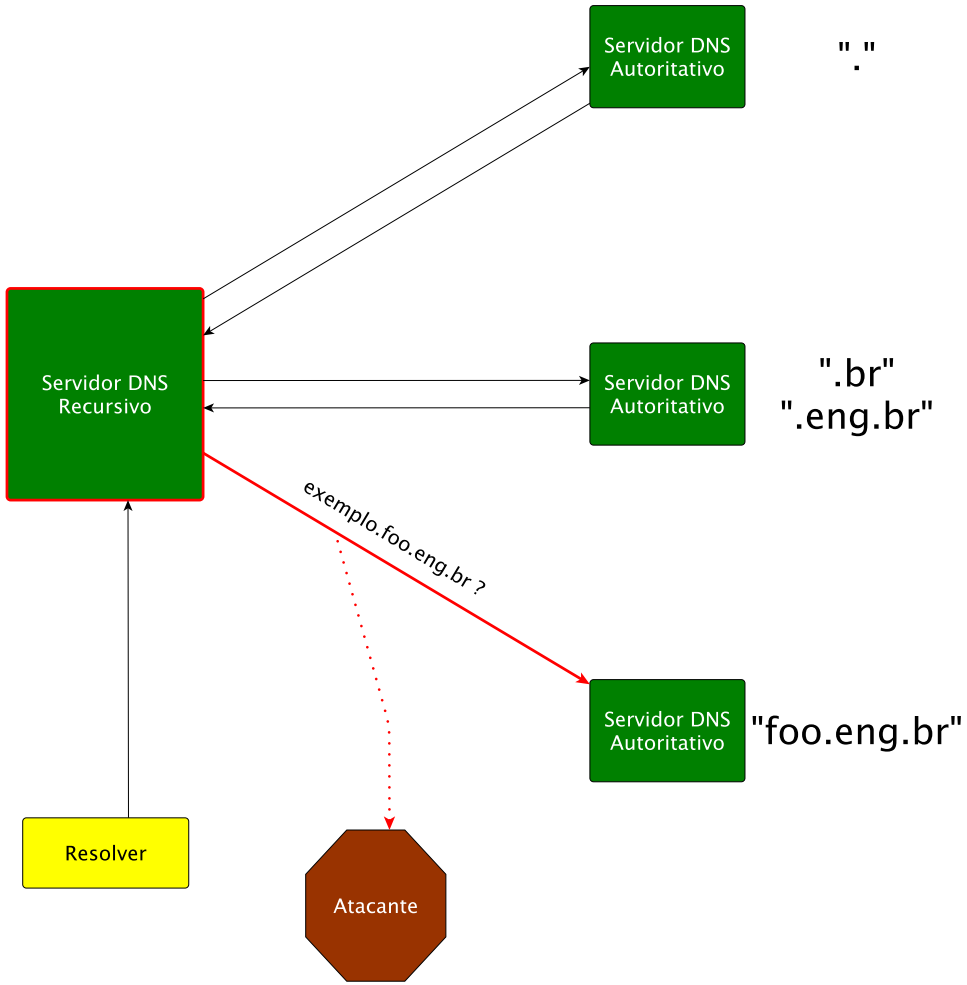
Exemplo de Ataque

Poluição de Cache



Exemplo de Ataque

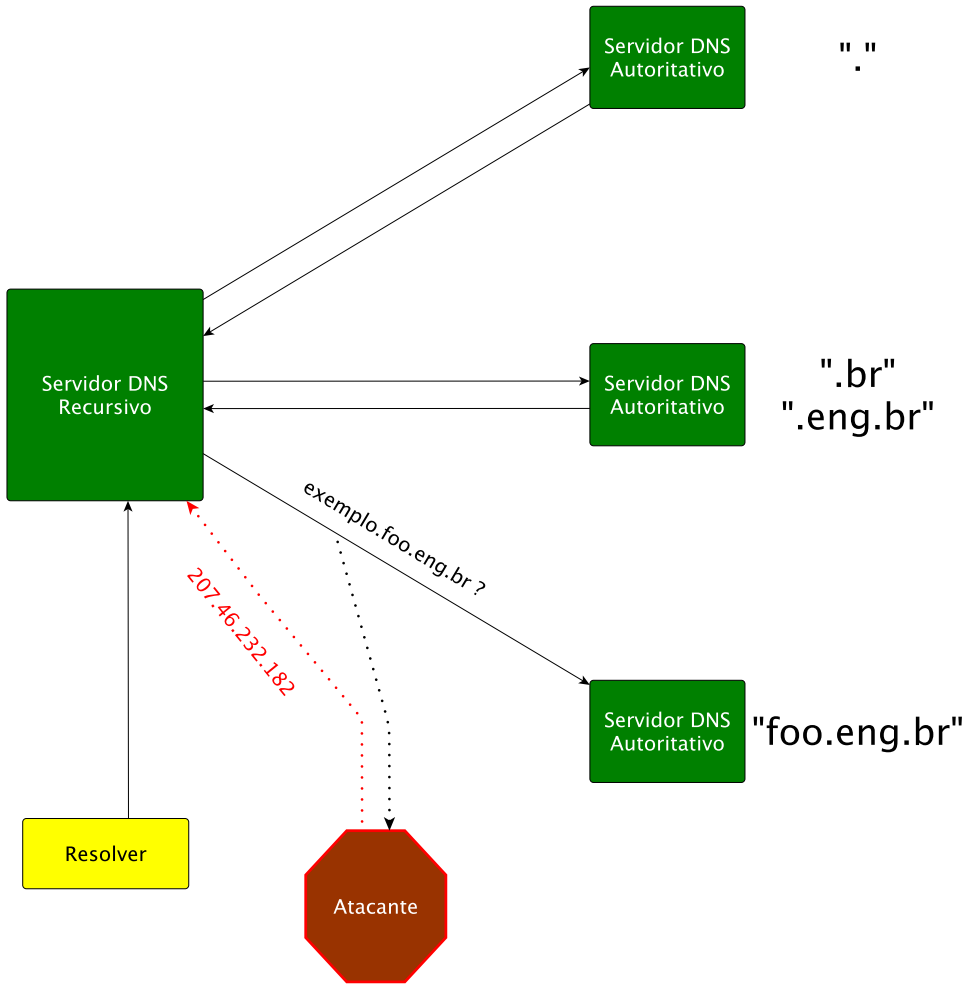
Poluição de Cache



Exemplo de Ataque

Poluição de Cache

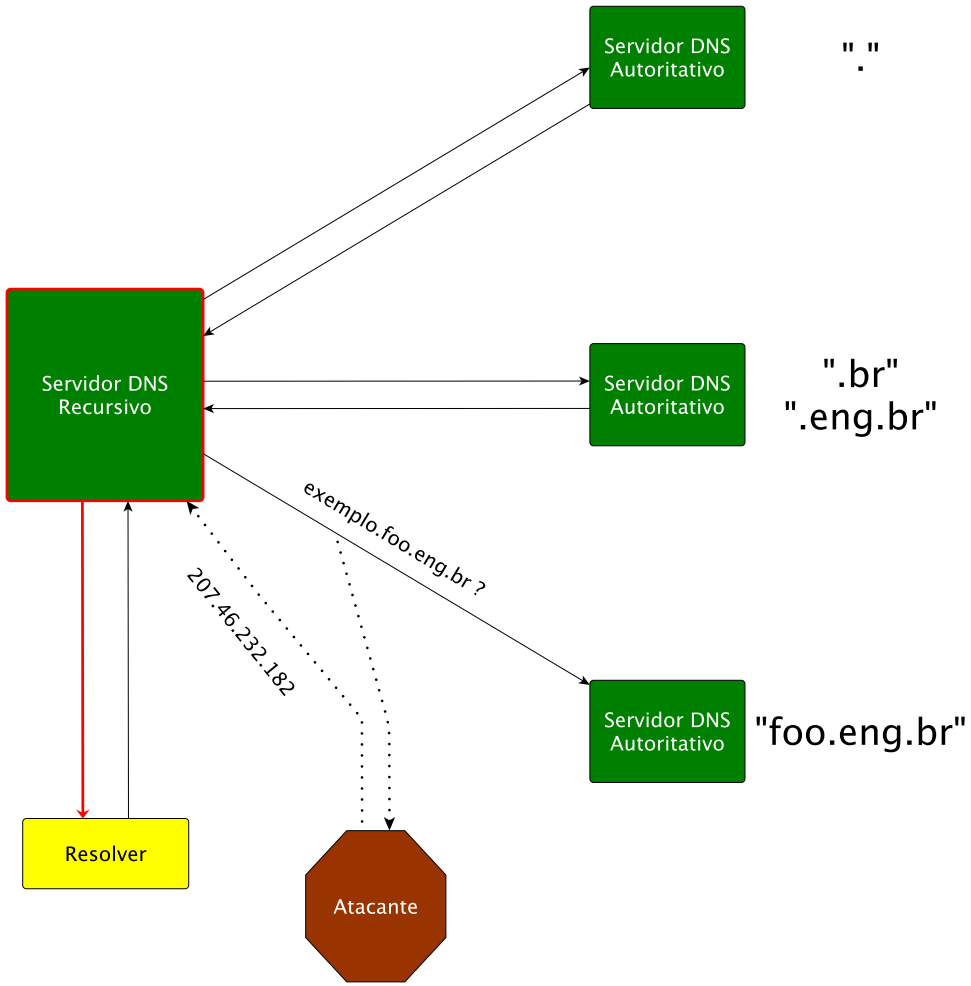
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque

Poluição de Cache

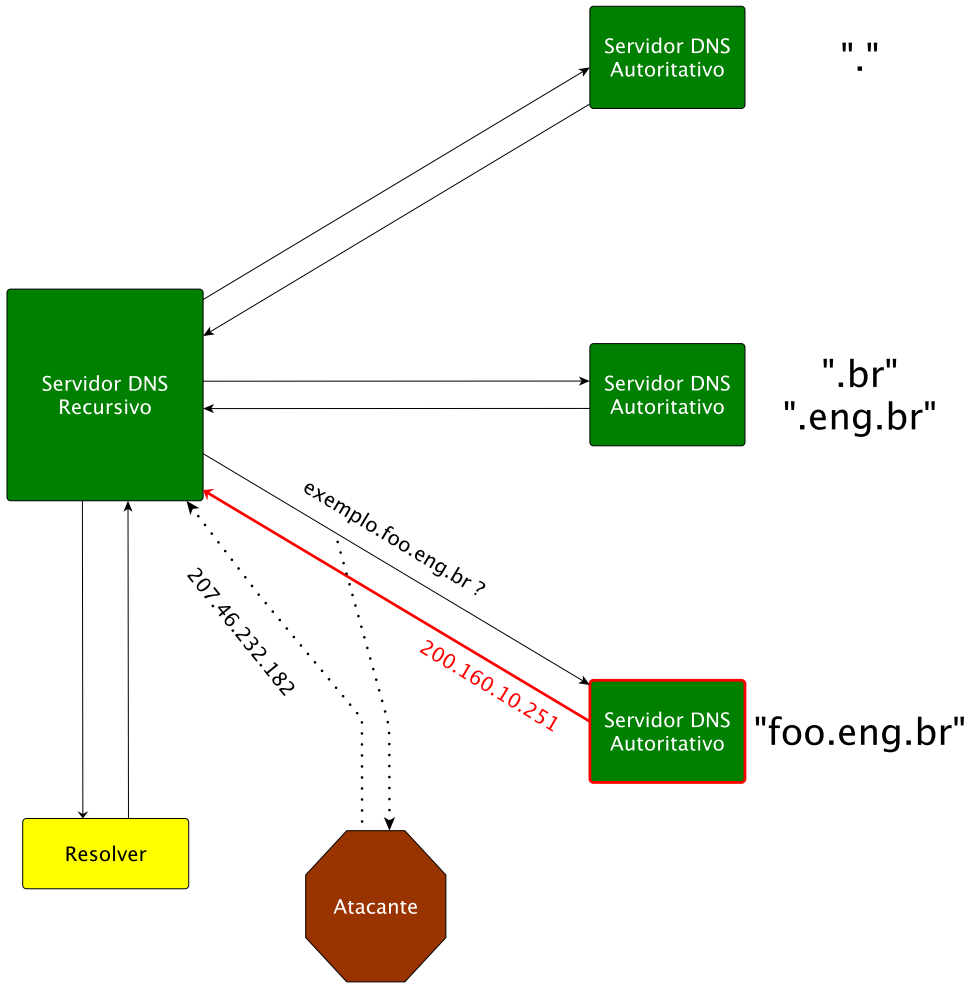
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque

Poluição de Cache

O atacante responde mais rápido, spoofando endereço do autoritativo



DNSSEC

Domain Name System SECurity extensions

- Extensão da tecnologia DNS
  (o que existia continua a funcionar)
- Possibilita maior segurança para o usuário na Internet
  (corrige falhas do DNS)

Garantias do DNSSEC

- Origem (Autenticidade)
- Integridade

Como configurar DNSSEC

Como configurar DNSSEC no seu dominio (servidor autoritativo)

- ftp://ftp.registro.br/pub/doc/configuracao_dnssec_dominio.pdf

Como configurar DNSSEC no servidor recursivo

- ftp://ftp.registro.br/pub/doc/configuracao_dnssec_servidor_recursivo.pdf

Mais informações podem ser encontradas nos tutoriais de DNS e DNSSEC:
https://registro.br/tecnologia/dnssec/tutoriais/

Perguntas?

http://registro.br/tecnologia/dnssec/tutoriais/

Envie suas dúvidas para tutorial-dnssec@registro.br