Grupo de Resposta a Incidentes de Segurança

Segurança DNS

Guilherme Iria

Sumário

- Introdução
  - O que é?
  - Qual a utilidade?
  - Como funciona?

- Ameaças
  - Amplification
  - Cache Poisoning
    - Derivações

- Medidas de proteção
  - Prevenção
  - Protocolos e extensões
  - Outras alternativas

Introdução – O que é ?

O que é DNS?

DNS(Domain Name System)

Protocolo com funções que visam associar informações a domínios de nomes

Introdução – Qual é sua utilidade ?

Quando você digita no navegador, por exemplo :

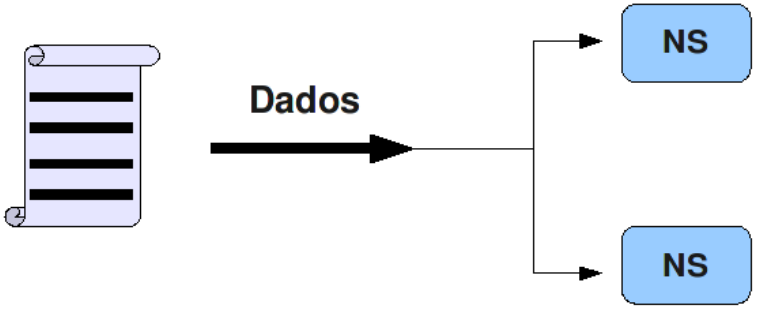
www.gris.dcc.ufrj.br

O nome é traduzido para o IP 146.164.3.48

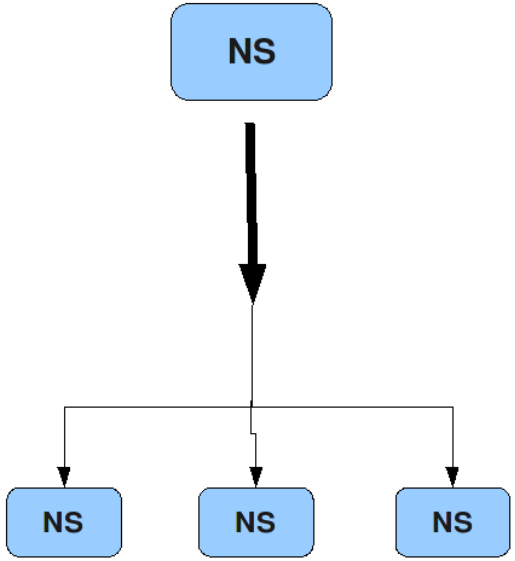
Este sim é o endereço do servidor web do GRIS.

Introdução – Como funciona ?

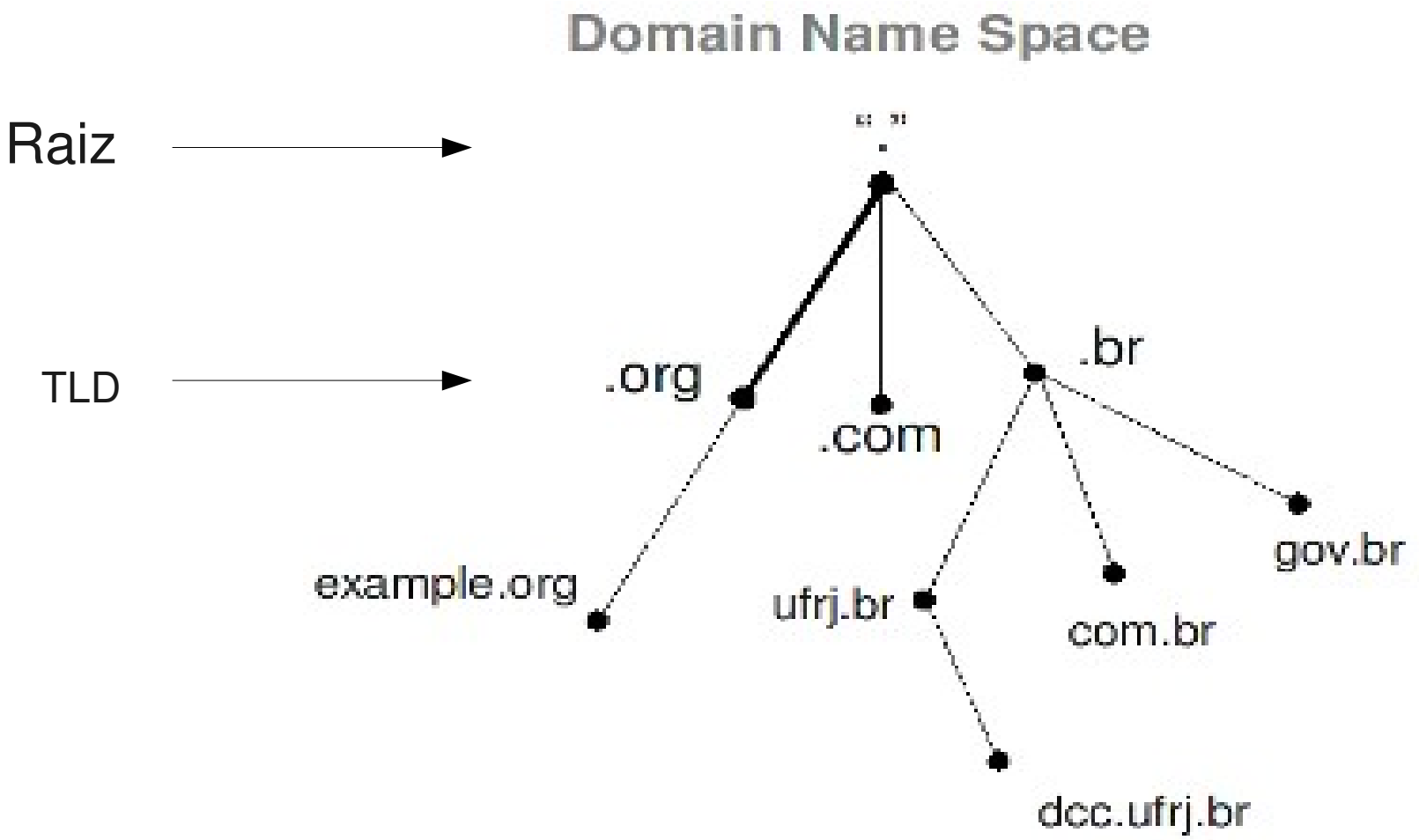
Dados distribuídos



De forma hierarquizada

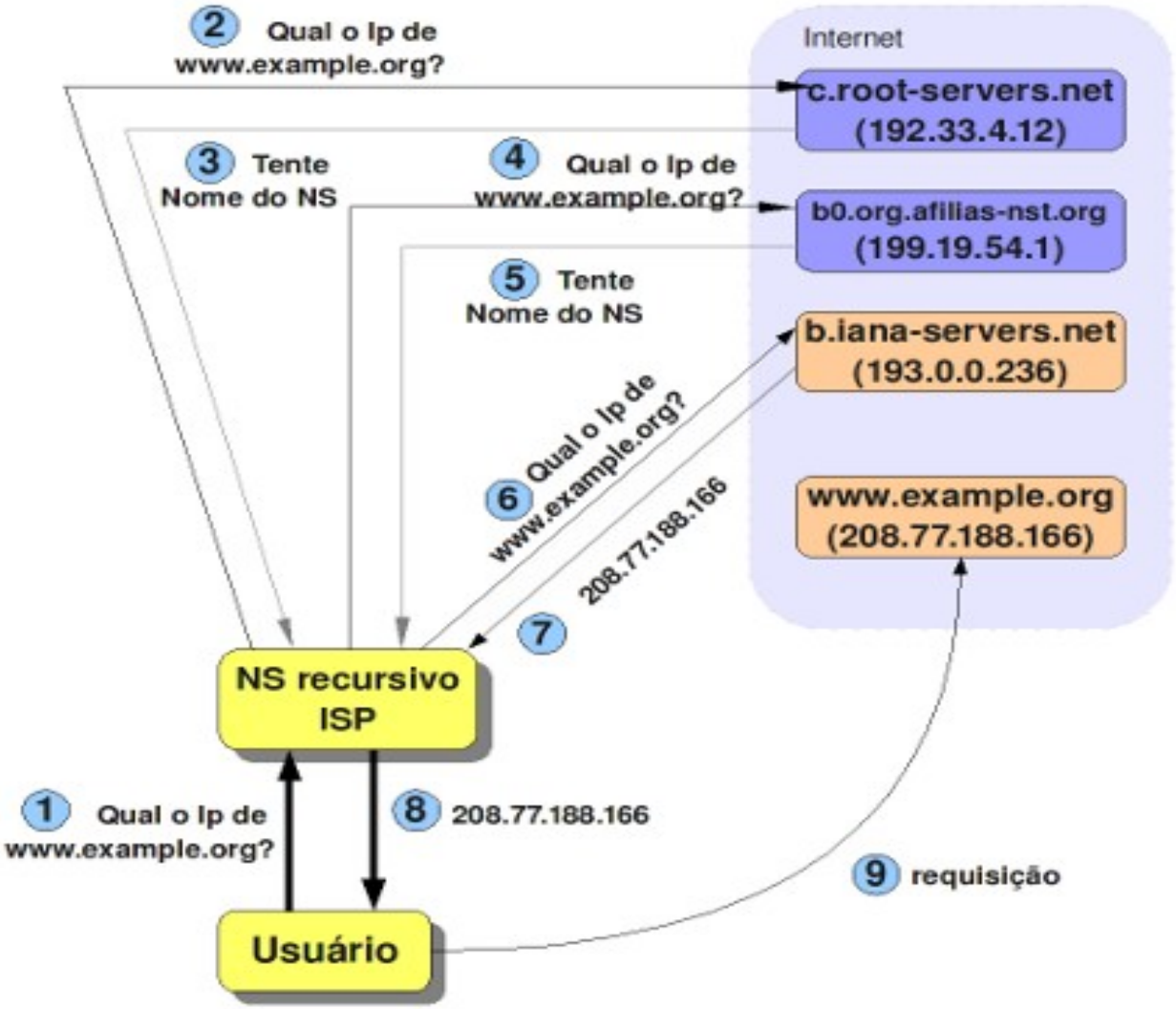


Introdução – Como funciona ?

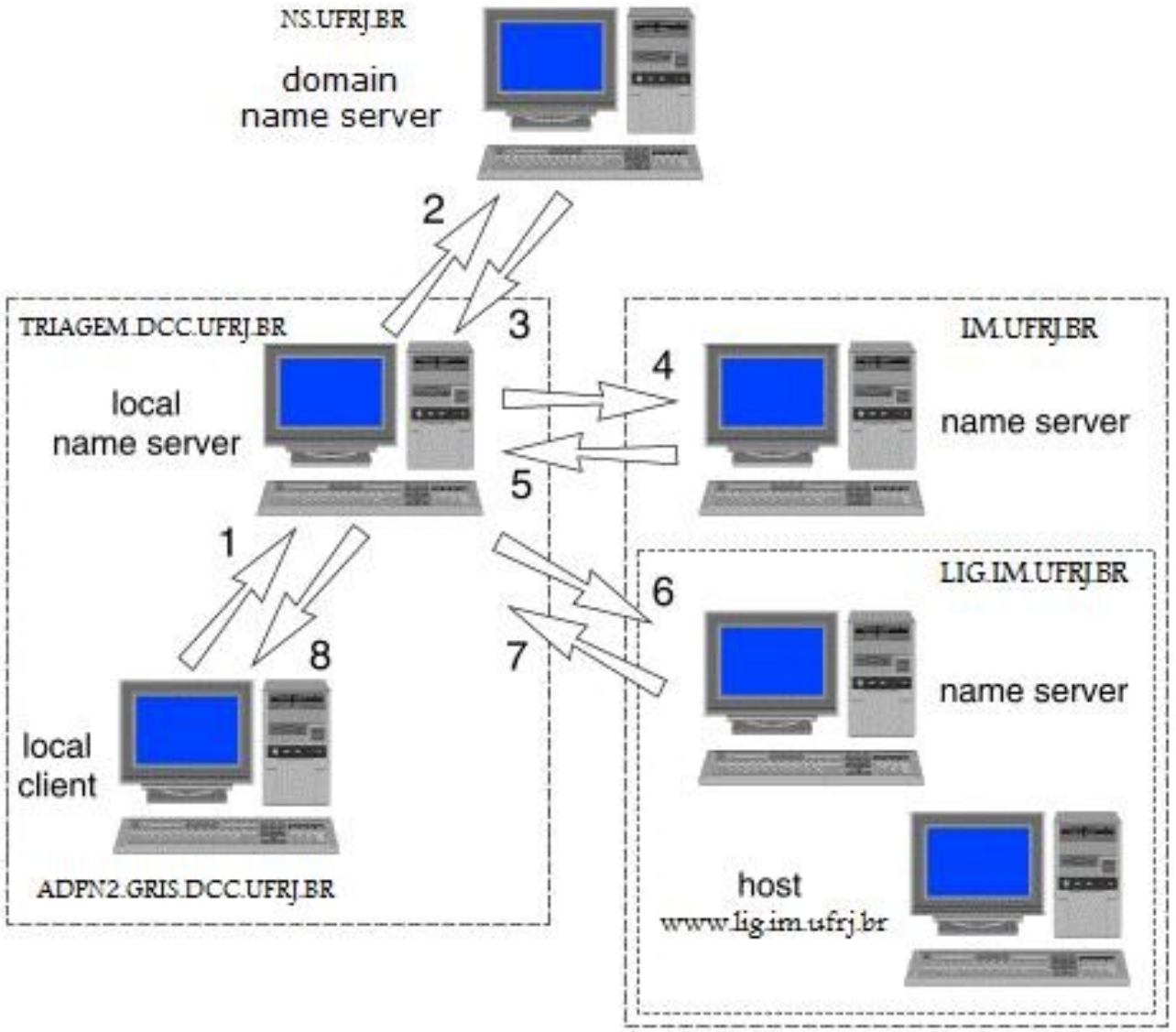


Introdução – Como funciona ?

Consultas



Introdução – Como funciona ?



Introdução – Como funciona ?

Name Servers

Respondem à consultas com autoridade
Delegação da zonas
Servidor primário e secundário
RR's (Registros de Recursos)

SOA: Especifica o servidor delegado para a zona.
A: Traduz um nome de máquina para um IPv4.
NS: Especifica o(s) endereço(s) IP do(s) servidor(es) de nome.
CNAME: Cria apelidos (alias) para o nome de uma máquina.
PTR: Traduz um endereço IP para um nome de máquina, possibilitando uma reverse lookup.
MX: Roteamento de e-mail. Traduz para o endereço do servidor de e-mail responsável do domínio.
Entre outros.

Introdução – Como funciona ?

Cache

- Agiliza consultas futuras e de outros usuários
- ttl(*time-to-live*) define o tempo de permanência no cache
- RR's possuem seus próprios ttl's

Introdução – Como funciona ?

Dependência circular

- Qual a resposta do servidor responsável pelo tld .br à consulta por www.ufrj.br?

- É necessário mais de um RR para evitar uma dependência circular.

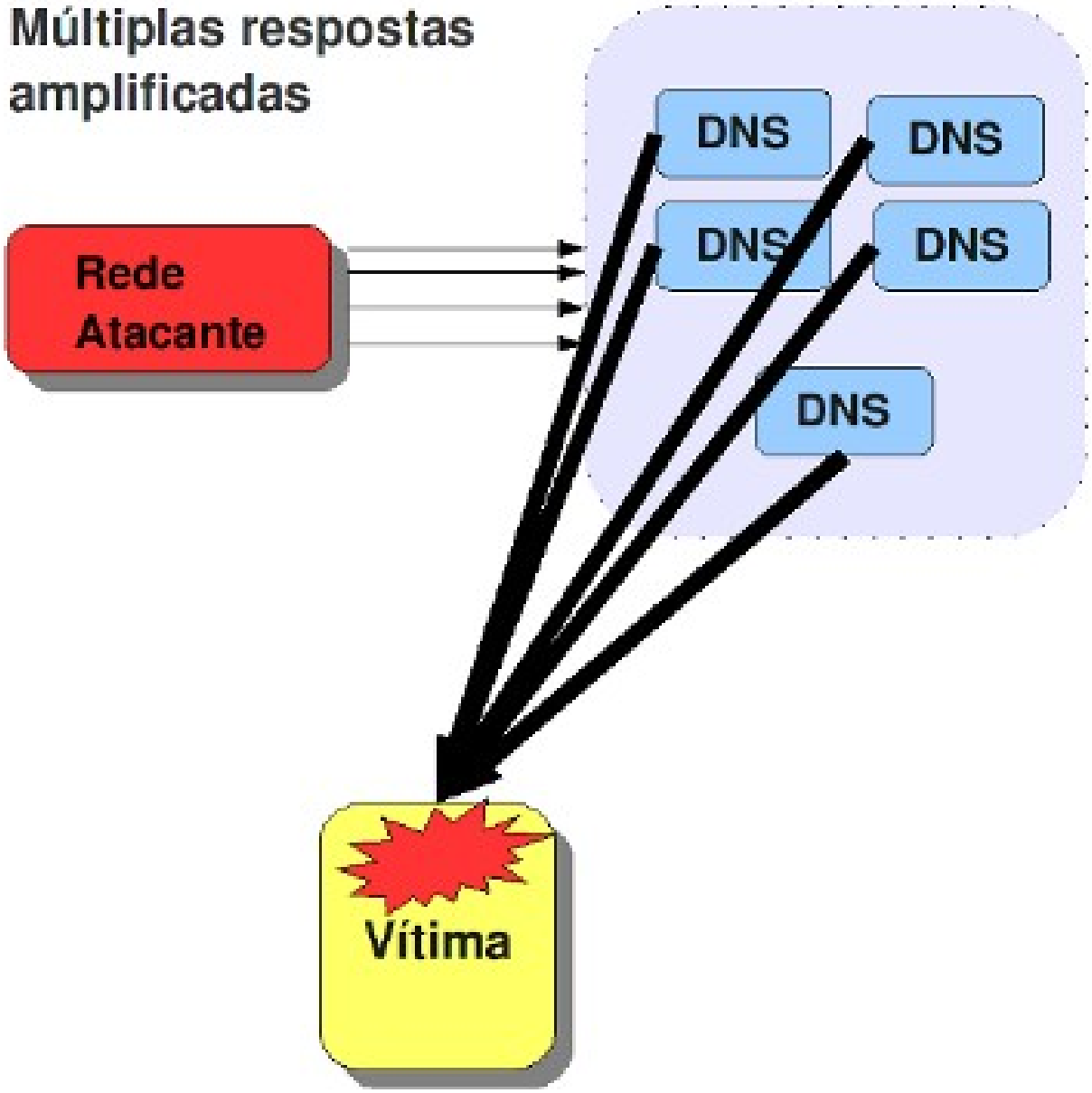
- No caso são passados registros adicionais, que podem ser RR's diferentes.

Ameaças – Introdução

Considerações sobre o protocolo:

- Protocolo de transporte: UDP ou TCP
- Porta do serviço : 53/udp 53/tcp
- Porta de origem da requisição
- QID(query identification)
- Verificação de fronteira: Registros adicionais fazem referência a uma zona autorizada?

Ameaças – DNS Amplification



Ameaças – DNS Amplification

O que acontece?

- Rede atacante faz requisições para servidores DNS abertos
- IP de origem das requisições é forjado (ip spoofing) para o ip da vítima
- A requisição é feita de forma a gerar uma resposta “maior” do servidor requisitado

Ameaças – DNS Amplification

E aí?

- Ataques de DDoS a partir de servidores mal configurados
- Difícil identificação do(s) atacante(s) reais
- Uma requisição de 60 bytes pode gerar uma resposta de até 4000 bytes

Ameaças – Cache Poisoning

Ocorre quando as entradas armazenadas em cache no NS não são as que correspondem à realidade.

Com isso, clientes contactarão servidores definidos arbitrariamente por um atacante.

Tráfego web, e-mail e dados de rede importantes estarão comprometidos

Pode afetar todos os clientes do servidor.

Ameaças – Cache Poisoning

Quando uma consulta é feita, o cliente aguarda uma resposta que deve coincidir com alguns atributos:

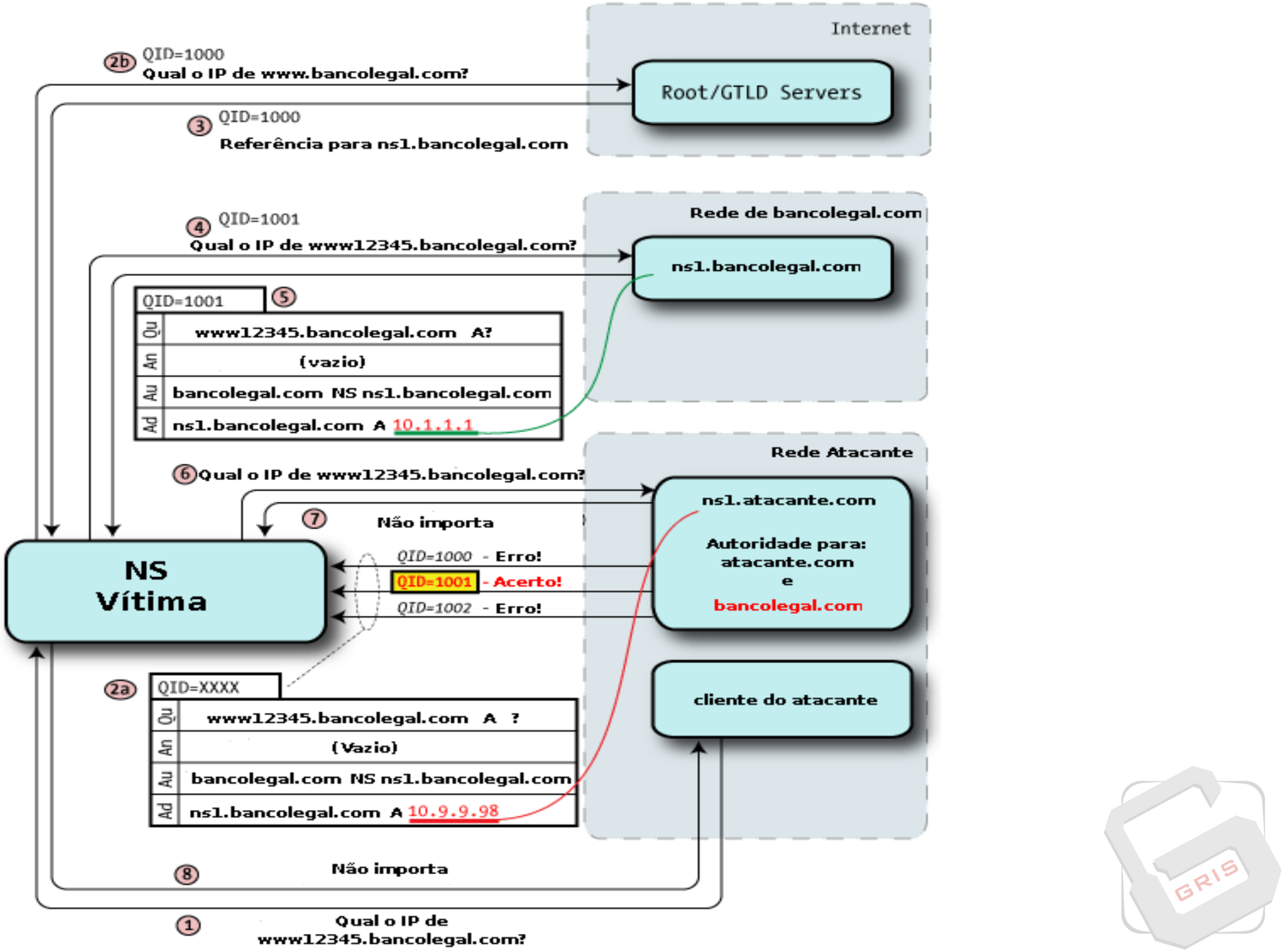
- Deve voltar ao mesmo IP que enviou a consulta
- A pergunta deve ser a mesma
- Deve voltar à mesma porta de origem
- O QID deve ser o mesmo

Ameaças – Cache Poisoning

As principais medidas corretivas para evitar ataques desse tipo se concentraram nos 2 últimos itens do slide anterior.

Em julho de 2008 o pesquisador Dan Kaminsky identificou formas mais efetivas de enviar sucessivas requisições a um servidor(flood), e conseguir que respostas forjadas sejam aceitas.

O que contribuiu para isso foi o fato de que os 2 itens citados não são gerados de forma aleatória satisfatoriamente.


Internet
Root/GTLD Servers
2b QID=1000
Qual o IP de www.bancolegal.com?
3 QID=1000
Referência para ns1.bancolegal.com
Rede de bancolegal.com
ns1.bancolegal.com
4 QID=1001
Qual o IP de www12345.bancolegal.com?
QID=1001
5
Qu www12345.bancolegal.com A?
An (vazio)
Au bancolegal.com NS ns1.bancolegal.com
Ad ns1.bancolegal.com A 10.1.1.1
Rede Atacante
6 Qual o IP de www12345.bancolegal.com?
ns1.atacante.com
Autoridade para:
atacante.com
e
bancolegal.com
7 Não importa
QID=1000 - Erro!
QID=1001 - Acerto!
QID=1002 - Erro!
NS
Vítima
cliente do atacante
2a
QID=XXXX
Qu www12345.bancolegal.com A ?
An (Vazio)
Au bancolegal.com NS ns1.bancolegal.com
Ad ns1.bancolegal.com A 10.9.9.98
8 Não importa
1 Qual o IP de
www12345.bancolegal.com?

Ameaças – Cache Poisoning

Neste ataque o servidor deve fazer uma consulta a um host inexistente de um domínio válido.

Nesse instante o atacante começa as tentativas de acertar a QID e a porta de origem. Em termos computacionais, o QID de 16 bits e a as possibilidades das portas de origem, a faixa de possibilidades NÃO é satisfatoriamente ampla. (Birthday attack).

Se a resposta for aceita, é armazenada em cache com um TTL definido pelo atacante(geralmente grande) e pode afetar vários RR's.

A com isso, uma das grandes preocupações era a de que o ataque poderia afetar também as entradas para um servidor TLD.

Ameaças – Outras

Transferência de zona

A atualização de informações para uma zona secundária é feita através da transferência de zona. Se alguém não autorizado realizar tal operação, terá acesso à informações sensíveis.

Pharming Drive by

Pharming é o direcionamento para um sistema fraudulento ao tentar acessar um sistema legítimo. Isso pode ocorrer alterando o arquivo HOSTS localmente, com cache poisoning, ou pela mudança do servidor que será consultado(resolver) para um fraudulento - drive by.

Medidas de Proteção

Algumas medidas preventivas que devem ser tomadas para proteger sistemas de possíveis ataques :

- Manter atualizado seu software, aplicar correções do fabricante.
- Restringir os clientes, se possível a somente clientes locais de sua rede.
- Desabilitar a recursão para consultas feitas por servidores não confiáveis.
- Restringir transferência de zona somente para o ip dos servidores envolvidos

Medidas de Proteção

Protocolos e extensões

Algumas medidas foram tomadas pela comunidade,
de modo a trazer segurança ao protocolo.

Uma dessas medidas foi a criação da suíte DNSSEC(DNS Security Extensions).
Seu propósito é o de tornar o protocolo mais seguro evitando ataques de cache poisoning, por exemplo, com o intuito de prover :

i)Autenticidade da origem de dados DNS
ii) Integridade de dados
iii)Não existência de um nome ou tipo

Medidas de Proteção

Protocolos e extensões

Porém não provê:
i) Confidencialidade de dados
ii) Proteção contra DDoS

Gera um problema com a enumeração de zona, fornece informações sensíveis que não são fornecidas com a implementação padrão do protocolo.

Além de não ser largamente difundido devido à sua complexidade de implementação.

Medidas de proteção

Outras alternativas:

Servidores recursivos abertos:

- OpenDNS
- DNS Advantage

Servidores root alternativos (aos do ICANN):

- OpenNIC

Dúvidas?

Referências

rfc 1034 - DOMAIN NAMES - CONCEPTS AND FACILITIES
rfc 1035 - DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
rfc 2671 - Extension Mechanisms for DNS (EDNS0)

An Illustrated Guide to the Kaminsky DNS Vulnerability - http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
Understanding Kaminsky's DNS Bug - http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug
DNS from Rocket Scientists - http://www.zytrax.com/books/dns/

Referências

Understanding how DNS works-
http://articles.techrepublic.com.com/5100-10878_11-1053442.html?tag=
DNS-Amplification-Attacks -
http://www.isotf.org/news/DNS-Amplification-Attacks.pdf
DNS Amplification Variation Used in Recent DDoS Attacks -
http://www.secureworks.com/research/threats/dns-amplification/
Tutorial DNSSEC
ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf

Obrigado!