UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

GUSTAVO SPIER LANDTRETER

dnstrace: Uma Ferramenta de Medição Ativa para Análise do Nível de Centralização do DNS da Internet

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação

Orientador: Prof. Dr. Lisandro Granville

Porto Alegre
2018

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer ao meu orientador, Lisandro Granville, por todo o auxílio e incentivo prestados durante a execução deste trabalho. Gostaria também de agradecer à Professora Luciana Nedel, que me introduziu ao mundo acadêmico.

Aos colegas do grupo de redes, meus sinceros agradecimentos por todo o auxílio prestado. Pela troca de ideias e palavras de incentivo quando precisei. Gostaria de expressar minha gratidão especialmente ao Arthur Jacobs, ao Luciano Zembruski e ao Giovane Moura.

A todos os meus colegas de faculdade, que compartilharam comigo desde os momentos difíceis de estudos na biblioteca e trabalhos noite adentro, até os momentos bem humorados nos corredores do INF.

Gostaria de agradecer à toda a minha família, em especial à minha mãe, Rachel, e à minha vó, Asta, que me deram suporte durante toda a minha trajetória. Ao Waldir, por me ajudar nos momentos em que mais precisei.

Agradeço também à Thayse, por todo o amor e suporte que ela me deu. A sua ajuda durante os momentos de desorganização, naqueles em que a inércia era maior do que a vontade, me mostraram que vale a pena batalhar por aquilo que queremos.

Também gostaria de agradecer, especialmente, ao Professor Raul Fernando Weber. Seus ensinamentos e memória permanecerão presentes na mente daqueles que tiveram o privilégio de cruzar o seu caminho.

RESUMO

O Sistema de Nomes de Domínio (*Domain Name System*) é um dos pilares da internet e já foi alvo de diversos ataques distribuídos de Negação de Serviço (*Distributed Denial of Service - DDoS*) ao longo dos anos. Como contra medida, a infraestrutura do DNS é projetada com uma série de mecanismos de replicação, tais como o uso de uma arquitetura distribuída de servidores DNS autoritativos e *IP Anycast*. Apesar da existência destas medidas, já foi possível observar que, quando sites dependem de um provedor terceirizado de serviços de DNS, é possível existir um certo nível de compartilhamento de infraestrutura. Nesse caso, há o risco de que um ataque destinado a um servidor DNS possa afetar outros servidores DNS que estejam compartilhando a sua infraestrutura com a do servidor alvo. No entanto, medir tais níveis de compartilhamento de infraestrutura é uma tarefa desafiadora, tendo em vista que a maioria dos pesquisadores tipicamente não têm acesso aos dados internos de provedores de DNS. Neste trabalho, apresentamos uma metodologia e uma ferramenta à ela associada - *dnstrace* - que permite medir, tanto o grau de centralização como o grau de compartilhamento da infraestrutura de DNS, utilizando medições ativas. Como estudo de caso, foram analisados os servidores de DNS autoritativos de todos os domínios presentes na lista *Alexa's Top 1 Million*, que reúne o 1 milhão de sites mais acessados na Internet. Os resultados mostram que, em alguns casos, até 12.000 servidores autoritativos de DNS compartilham a mesma infraestrutura de base de um provedor de DNS terceirizado. Portanto, na eventualidade de algum ataque, estes servidores autoritativos correm maior risco de serem afetados por danos colaterais.

Palavras-chave: DNS. Compartilhamento de Infraestrutura. DDoS. Danos Colaterais.

ABSTRACT

The Internet Domain Name System (DNS) is one of the pillars for the Internet and is the subject of various Distributed Denial-of-Service (DDoS) attacks along the years. As a counter measure, the DNS infrastructure has been engineered with a series of replication measures, such as relying on multiple authoritative name servers and using IP anycast. Even though these measures have been in place, we have seen that, when websites rely on third-party DNS providers for authoritative services, there may be certain levels of infrastructure centralization. In this case, there is a risk that an attack against a DNS target might affect other DNS name servers sharing part of the infrastructure with the intended victim. However, measuring such levels of infrastructure sharing is a daunting task, given that researchers typically do not have access to DNS provider internals. In this work, we introduce a methodology and associated tool - *dnstrace* - that allows measuring, to various degrees, the level of both concentration and infrastructure sharing using active DNS measurements. As a case study, the authoritative name servers of all domains of the Alexa Top 1 Million most visited websites were analyzed. The results show that, in some cases, up to 12.000 authoritative name servers share the same underlying infrastructure of a third-party DNS provider. As such, in the event of an attack, those authoritative servers have increased risk of suffering from collateral damage.

Keywords: DNS, Infrastructure Sharing, Collateral Damage, DDoS.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AS	Autonomous System
ASN	Autonomous System Number
DDoS	Distributed Denial-of-Service
DNS	Domain Naming System
DPN	Domínio de Primeiro Nível
DSN	Domínio de Segundo Nível
FQDN	Fully Qualified Domain Name
HBTL	Hop Before the Last
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IP	Internet Protocol
JDK	Java Development Kit
JNI	Java Native Interface
JSON	JavaScript Object Notation
MVC	Model View Controller
ORM	Object-Relational Mapping
PID	Process Identifier
REST	Representational State Transfer
TTL	Time to Live
URI	Uniform Resource Identifier

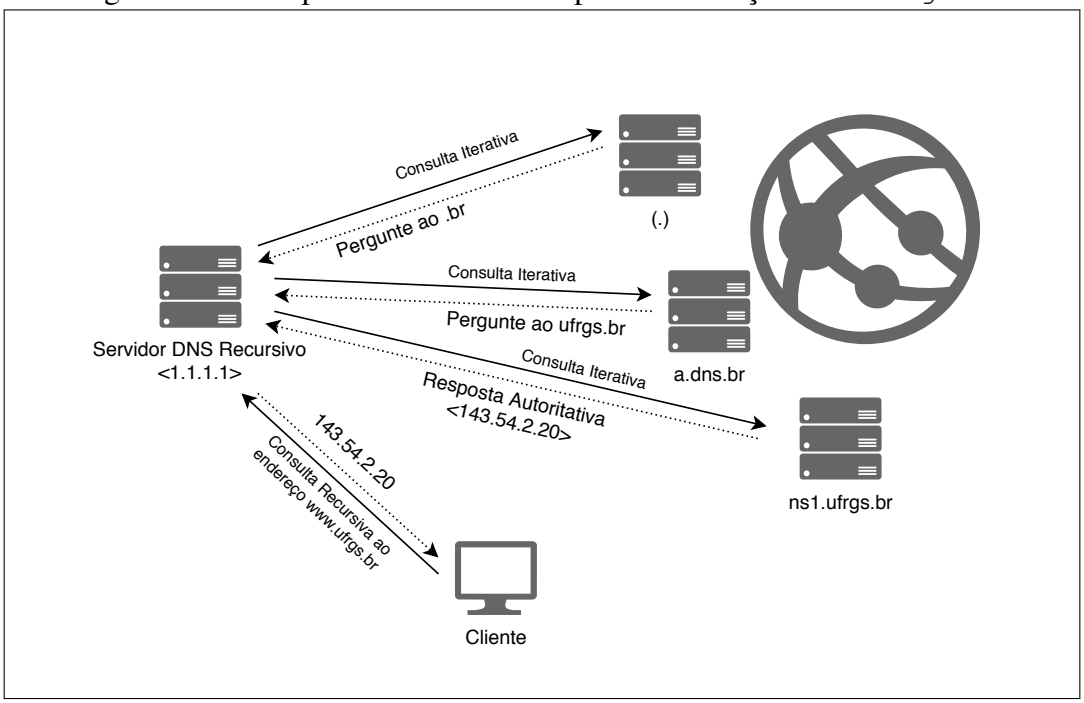
SUMÁRIO

1 INTRODUÇÃO

O Sistema de Nomes de Domínio (*Domain Name System - DNS*) da Internet estabelece um espaço de nomes hierárquico global que permite o mapeamento de nomes de máquina, redes e serviços para endereços IP (MOCKAPETRIS, 1987). Tendo em vista este papel, o DNS constitui um dos pilares da Internet. Clientes conectados à Internet a partir de qualquer lugar do mundo utilizam servidores DNS para resolver os endereços IP associados a um nome de domínio. Por exemplo, para resolver o domínio `ufrgs.br`, um cliente envia uma chamada de consulta ao seu servidor DNS Recursivo, que é um servidor DNS capaz de resolver, por ele, um nome de domínio. Servidores de DNS Recursivos são, por sua vez, responsáveis por direcionar esta consulta a um servidor DNS *Autoritativo*. Um servidor DNS Autoritativo é aquele que, através de sua base local de conhecimento, conhece o conteúdo de uma zona DNS e pode responder consultas relacionadas à ela (ELZ et al., 1997).

Por exemplo, um cliente pode enviar uma consulta ao endereço `1.1.1.1` - um servidor DNS Recursivo público - solicitando o endereço IP associado ao endereço `www.ufrgs.br`. O servidor recursivo vai, em nome do usuário, direcionar a consulta a um dos servidores autoritativos responsáveis pelo domínio `ufrgs.br`, neste caso, `ns1.ufrgs.br` ou `ns2.ufrgs.br`. Os servido autoritativo irá então consultar sua base local e retornará o IP associado ao domínio ao servidor DNS Recursivo, que irá responder a consulta ao cliente.

Figura 1.1: Exemplo de consulta DNS para o endereço `www.ufrgs.br`



Fonte: Autor

Devido à sua importância para o funcionamento da Internet, os servidores DNS Autoritativos têm sido vítimas frequentes de ataques Distribuídos de Negação de Serviço (*Distributed Denial-of-Service - DDoS*). Os servidores raiz do DNS, conhecidos como *DNS Root Servers*, autoritativos à zona hierárquica raiz (.) do DNS (*DNS Root Zone*), têm sido alvo de diversos ataques na última década (Root Server Operators, 2015; Root Server Operators, 2016; Weinberg, M., Wessels, D., 2016; MOURA et al., 2016a; SENGUPTA, 2012). Outros servidores DNS autoritativos também podem ser alvos de ataque. Em 2016, um dos maiores provedores de DNS da Internet, Dyn, foi vítima de um ataque onde sua rede foi sobrecarregada com um fluxo de dados de 1.3Tb/s, originado a partir de uma *botnet* de dispositivos *IoT* infectados com o *malware Mirai* (HILTON, 2016). Este ataque impactou a operação de diversos *websites* que utilizavam os serviços da Dyn, incluindo o *Twitter*, *Netflix*, *PayPal* e o do jornal *The New York Times* (PERLROTH, 2016).

Na tentativa de frear estes ataques, o DNS foi projetado levando em conta uma arquitetura distribuída, com diversas camadas de replicação: um domínio pode, por exemplo, utilizar diversos servidores DNS autoritativos (como é o caso da UFRGS). Além disso, os administradores de rede podem utilizar outras técnicas, tais como o emprego de *IP Anycast* (MCPHERSON et al., 2014), que permite que o mesmo endereço IP seja atribuído e anunciado a partir de diversos locais dispersos geograficamente. Cada um destes locais pode, por sua vez, empregar balanceadores de carga em sua rede local, dis-

tribuindo consultas entre vários servidores DNS (MOURA et al., 2016a), aumentando a confiabilidade do sistema.

Embora estas medidas estejam sendo utilizadas, pode-se perceber que, quando nomes de domínio utilizam o mesmo provedor DNS, eles podem estar (sabendo ou não) compartilhando diferentes níveis de infraestrutura. Este modelo de compartilhamento pode tornar-se um problema quando um ataque DDoS de larga escala está ocorrendo: caso um servidor DNS gerenciado pelo provedor seja alvo do ataque, e alguma parte desta infraestrutura compartilhada fique sobrecarregada, todas as zonas DNS gerenciadas pelo provedor podem ser impactadas. Consequentemente, várias zonas de domínio podem também tornar-se inacessíveis, mesmo não sendo o alvo original do ataque. O ataque sofrido pela Dyn exemplifica o risco de *"danos colaterais"* quando servidores DNS autoritativos que estejam compartilhando a sua infraestrutura são alvos de ataque.

Medir a extensão na qual esta infraestrutura está sendo compartilhada, no entanto, é uma tarefa desafiadora. Grupos de pesquisa normalmente não possuem acesso à estrutura e organização interna dos provedores de serviços DNS. Por conta disso, torna-se necessário partir para uma abordagem de medições que permita estimar, em nível de endereços IP, se existe um certo nível de compartilhamento de infraestrutura. Um destes trabalhos foi conduzido por Allman (ALLMAN, 2018), onde o autor analisa dados históricos dos arquivos de zona DNS para os domínios `.com`, `.org` e `.net`, cobrindo um período de nove anos. O autor analisa o nível de compartilhamento de infraestrutura entre servidores DNS autoritativos. Dentre suas descobertas, Allman mostra que, por exemplo, um único servidor autoritativo pode ser responsável por até 9.000 zonas DNS. Esse estudo, no entanto, focou-se em explorar o compartilhamento de infraestrutura no nível de IP de servidores autoritativos, ou seja, buscou observar quantos domínios estavam sendo gerenciados por um mesmo servidor. Mesmo assim, os autores ressaltam no estudo que o compartilhamento de recursos de infraestrutura, em nível de rede, está se tornando uma prática cada vez mais comum. No entanto, eles não realizam nenhuma investigação em relação ao compartilhamento de infraestrutura em nível de Sistemas Autônomos (AS), em casos onde estes dependam exclusivamente do serviço de terceiros para a hospedagem de DNS. Adicionalmente, também não foi realizada nenhuma análise do compartilhamento de infraestrutura de servidores DNS autoritativos para Nomes de Domínio Completamente Qualificados (do inglês, *FQDN*, ou *Fully Qualified Domain Names*), como por exemplo, `www.ufrgs.br`.

Tendo em vista este cenário, o presente trabalho tem como objetivo desenvol-

ver uma metodologia que permita medir, em diversos níveis, o grau de concentração e de compartilhamento de infraestrutura de servidores DNS autoritativos, realizando medições ativas em servidores DNS. O trabalho é focado em analisar uma possível centralização na quantidade de *FQDNs* gerenciados por Sistemas Autônomos da Internet. Adicionalmente, foi desenvolvida a ferramenta *dnstrace* - uma ferramenta de código aberto que implementa a metodologia proposta e fornece uma visão consolidada dos dados gerados. Como estudo de caso, a ferramenta *dnstrace* foi utilizada para analisar todos os domínios presentes na lista *Alexa's Top 1 Million* (Alexa, 2018), que reúne o 1 milhão de sites mais acessados da Internet. Foi possível mostrar que, em alguns casos, até 12.000 servidores DNS autoritativos, dentre os *websites* mais acessados da Internet, compartilham a mesma infraestrutura de base fornecida por provedores terceirizados, o que evidencia o risco de dano colateral entre estes servidores no caso de um ataque.

O texto está organizado da seguinte forma. No capítulo 2 são apresentados trabalhos relacionados. O capítulo reúne os estudos já realizados na análise do DNS e da sua estrutura. No capítulo 3, é descrita a metodologia desenvolvida, que permite a medição do compartilhamento de infraestrutura dos serviços DNS. São abordadas as tecnologias que envolvem essa medição e a sua eficiência. No capítulo 4, é apresentada a ferramenta *dnstrace*, bem como os detalhes de sua implementação. No capítulo 5, são apresentados os resultados obtidos durante o estudo de caso realizado com base na lista *Alexa's Top 1 Million*. No capítulo 6 são apresentadas as conclusões deste trabalho, além de trabalhos futuros.

2 TRABALHOS RELACIONADOS

Pesquisas focadas na realização de medições do sistema DNS da Internet já foram realizadas no passado, algumas relacionadas à robustez da infraestrutura DNS, outras analisando possíveis pontos de falha no seu ecossistema. Particularmente, ressaltam-se três estudos que fornecem evidências da existência de compartilhamento na infraestrutura DNS global e evidenciam os perigos que a envolvem.

Em 2016, Moura *et al.* (MOURA et al., 2016b) analisou um ataque DDoS destinado aos servidores raiz do DNS. Entre 30 de Novembro e 1°de Dezembro de 2015, percebeu-se um aumento no volume médio de requisições recebidas pelos servidores raiz do DNS. Durante este período, os servidores receberam um volume médio de requisições cem vezes maior do que o volume padrão. Os autores ressaltaram que, embora estes ataques não tenham sido direcionados a nenhum serviço específico, como por exemplo, um único web site, houve uma forte evidência de que vários serviços acessíveis pela Internet sofreram instabilidades, devido ao fato de compartilharem sua infraestrutura de base com os servidores alvos do ataque. Neste evento, alguns servidores responsáveis pelo TLD `.nl`, por exemplo, sofreram quedas devido ao dano colateral recebido durante o ataque aos servidores raiz do DNS. Embora esta pesquisa tenha realizado este diagnóstico e tenha concluído que a centralização dos serviços de DNS tenha uma parcela de participação nos efeitos colaterais sofridos por diversos serviços, ela não investigou, em detalhe, o nível de centralização da infraestrutura do DNS.

O estudo realizado por Bates *et al.* (BATES et al., 2018) propôs uma solução para medir o quão resiliente o serviço global de DNS permanece, tendo em vista o advento de soluções de hospedagem baseadas na nuvem que têm movido vários serviços para um modelo terceirizado de hospedagem, incluindo servidores DNS. Nesse trabalho, os autores analisaram a existência de uma tendência de centralização no DNS ao longo do tempo, com base em uma amostra de 1.000 domínios de web sites americanos fornecidos pela lista *Alexa Top Sites* (AMAZON, 2018). Com base nos domínios `.com`, `.net`, e `.org`, os autores evidenciaram a existência de um movimento de centralização, tendo em vista que estes domínios compõem os domínios de primeiro nível, ou DPNs, mais antigos da Internet. No entanto, os autores ressaltam que estes resultados podem ser diferentes caso outros DPNs sejam considerados na análise, como por exemplo, domínios `.ru` e `.cn`. Embora este estudo forneça um esboço no que tange à robustez do DNS, o trabalho não considerou os servidores DNS autoritativos, que representam um papel crucial para a

robustez do sistema. Este aspecto, no entanto, é abordado pelo presente trabalho.

Allman *et al.* (ALLMAN, 2018) conduziu um estudo para observar a robustez do ecossistema DNS. O estudo foi focado nos domínios de segundo nível, ou DSNs, (por exemplo, `ufrgs.br`). Nesse estudo, os autores utilizaram dados da zona DNS dos DPNs `.com`, `.net` e `.org`. Tais dados foram coletados durante um período de nove anos. Com base neles, foi realizada uma análise do grau de compartilhamento de infraestrutura do DNS. Inicialmente, percebeu-se que, dentre os dados analisados, de 91% a 93% dos domínios de segundo nível compartilham, pelo menos, um servidor DNS (por IP) com outro domínio. Também foi observado que metade dos domínios de segunda ordem compartilham exatamente o mesmo conjunto de servidores DNS com, pelo menos, outros 163 domínios de segunda ordem. Além disso, uma análise de compartilhamento de rede (por blocos de IP) também foi realizada. Nesta análise, pode-se observar que existe um nível ainda maior de compartilhamento de infraestrutura sob o ponto de vista de rede do que quando analisados os servidores individualmente. Os autores ressaltam que o compartilhamento de infraestrutura no nível de rede entre domínios está se tornando uma prática mais comum ao longo do tempo. O estudo também utilizou estes dados para analisar se o compartilhamento de infraestrutura é uma prática que ocorre com mais frequência entre domínios com maior ou pior *ranking*. Esta análise, no entanto, não apontou nenhuma tendência específica.

Considerando a pesquisa realizada até o momento pela comunidade acadêmica, há fortes evidências que sugerem uma tendência de centralização na infraestrutura do DNS. No entanto, nenhum dos trabalhos analisou a centralização, ou o grau de compartilhamento de infraestrutura, entre servidores DNS autoritativos. Da mesma forma, também não foi realizada, até então, nenhuma análise que relacione a centralização de servidores DNS autoritativos entre os Sistemas Autônomos que os gerenciam. Ambos aspectos serão abordados na metodologia apresentada a seguir.

3 METODOLOGIA

Como forma de identificar a ocorrência de compartilhamento de infraestrutura de servidores DNS autoritativos na Internet, a presente metodologia é focada na realização de medições ativas nos servidores DNS responsáveis pelos *websites* mais populares da internet, com base na lista *Alexa's Top 1 Million* (AMAZON, 2018).

Com o advento de serviços de hospedagem na nuvem, muitas empresas já não mantém suas próprias infraestruturas DNS, recorrendo à terceirização destes serviços em provedores externos. Tendo em vista este comportamento, identificar possíveis gargalos na infraestrutura DNS de diversos domínios distintos torna-se uma tarefa desafiadora. Além desta tendência, muitas empresas também começaram a anunciar seus próprios blocos de endereços IP a partir de *data centers* gerenciados por provedores de DNS terceirizados. Essa tendência pode estar criando um movimento de centralização no ecossistema DNS, onde *web sites* completamente não relacionados podem começar a sofrer danos colaterais originados de ataques DDoS, mesmo sem que estes sejam os alvos pretendidos do ataque.

Este risco de dano colateral não pode ser estimado simplesmente por uma análise direta dos endereços IP associados à servidores DNS autoritativos, tendo em vista que, diferentes servidores - cada um associado a um bloco de IP da empresa cuja zona ele gerencia - podem estar sendo suportados pela mesma infraestrutura de base de um provedor terceirizado. Além disso, pela natureza de negócio de provedores de serviços DNS, os dados necessários para realizar a análise de tal agregação raramente são publicamente divulgados. Esse risco pode, no entanto, ser medido caso seja possível encontrar um gargalo comum (ou ponto único de falha) na rota que leva a um dado conjunto de servidores remotos. Por exemplo, ao obter o endereço IP associado a `ns1.paypal.dynect.net` - um dos servidores DNS autoritativos para o domínio `paypal.com` - e examinar o seu Sistema Autônomo, observa-se que ele pertence a um provedor terceirizado. De fato, este servidor autoritativo está sendo mantido pela empresa *DynDNS*. Logo, caso outros servidores DNS estejam sendo hospedados sob esta mesma infraestrutura gerenciada pela *DynDNS*, eles começam a compartilhar o risco de danos colaterais na eventualidade de um ataque. Por esse motivo, é proposta uma abordagem que permita identificar estes gargalos através de uma implementação customizada da ferramenta `traceroute`. No capítulo 4, detalhamos a implementação customizada da ferramenta *traceroute*, bem como a arquitetura da ferramenta proposta.

3.1 Ferramental

Como forma de facilitar a descrição da metodologia proposta, são utilizadas as seguintes ferramentas comumente presentes no ecossistema *GNU/Linux*:

3.1.1 *dig*

A ferramenta **dig**, do inglês *Domain Information Groper* é uma ferramenta flexível para a realização de consultas a servidores DNS (CONSORTIUM, 2018a). É amplamente utilizada por administradores de rede devido à sua simplicidade. Com ela é possível, por exemplo, obter a relação de servidores DNS autoritativos a uma zona DNS. Também é possível realizar consultas a registros tipo A - que mapeiam um nome de domínio a um endereço IP. Ao executar o Código 3.1, é possível obter a lista de servidores autoritativos ao domínio `ufrgs.br`. O Código 3.3 exemplifica o uso da ferramenta **dig** para obter os registros DNS de tipo A associados ao nome `ns1.ufrgs.br`.

Código 3.1: Consulta aos servidores DNS autoritativos ao domínio `ufrgs.br`

```
user@localhost - ~$ dig ns ufrgs.br

; <<>> DiG 9.10.6 <<>> ns ufrgs.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44828
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0,
   ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ufrgs.br.      IN  NS

;; ANSWER SECTION:
ufrgs.br.   600 IN  NS  pampa.tche.br.
ufrgs.br.   600 IN  NS  ns2.ufrgs.br.
ufrgs.br.   600 IN  NS  ns1.ufrgs.br.

;; Query time: 8 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Oct 19 14:09:53 -03 2018
;; MSG SIZE  rcvd: 98{}
```

Código 3.2: Consulta a registros do tipo A para o endereço `ns1.ufrgs.br`

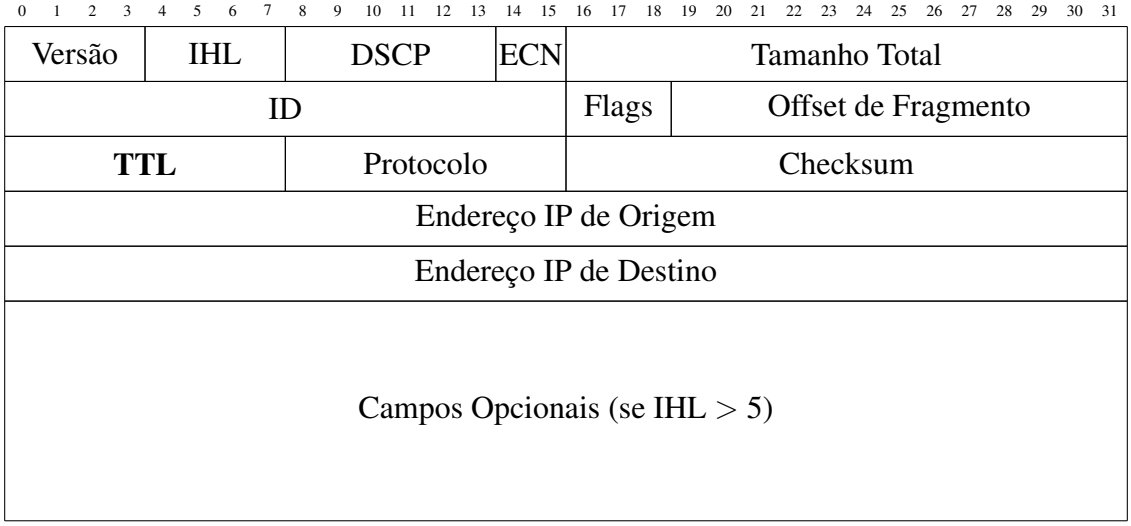
```
user@localhost - ~$ dig ns1.ufrgs.br

; <<>> DiG 9.10.6 <<>> ns1.ufrgs.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48185
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns1.ufrgs.br.      IN  A

;; ANSWER SECTION:
ns1.ufrgs.br.   600 IN  A 143.54.1.58

;; Query time: 7 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov 19 20:33:36 -02 2018
;; MSG SIZE  rcvd: 57
```

3.1.2 *traceroute*

A ferramenta **traceroute** é utilizada por administradores de rede para realizar o rastreamento da rota percorrida por pacotes IP a partir do servidor local até um servidor-alvo remoto (CONSORTIUM, 2018b). De forma a compreender o funcionamento da ferramenta, é necessário entender o funcionamento do campo *TTL*, presente no cabeçalho dos datagramas IP.

Figura 3.1: Cabeçalho de um datagrama IP



Fonte: (POSTEL, 1981b)

O campo **TTL**, do inglês *Time to Live*, representa o número máximo de saltos que um pacote IP pode sofrer, ou seja, o número máximo de roteadores que irão redirecionar um pacote até que o mesmo seja descartado. Roteadores que implementam o protocolo IP subtraem o valor do campo TTL em uma unidade antes de rotear cada pacote para seu

destino. Caso o valor do TTL chegue a zero, o pacote é descartado. De forma inteligente, a ferramenta *traceroute* utiliza este parâmetro para rastrear todos os roteadores participantes da rota de um pacote até o seu servidor de destino. A ferramenta realiza este processo da seguinte forma: o primeiro pacote enviado pela ferramenta para o servidor de destino possui, no seu cabeçalho, o campo TTL com valor 1. Dessa forma, o primeiro roteador que receber este pacote irá decrementar este valor em 1 unidade, e consequentemente descartar o pacote, respondendo ao endereço IP de origem. O segundo pacote será enviado pela ferramenta com o campo TTL com valor 2, e assim por diante, de forma consecutiva, até que ela receba uma resposta cuja origem é o servidor remoto alvo. Utilizando essa estratégia, a ferramenta *traceroute* consegue desenhar a rota percorrida por um pacote até o seu endereço de destino. O Código 3.3 demonstra o resultado da execução da ferramenta *traceroute* a partir de um servidor na rede da UFRGS, com destino a um servidor da USP.

Código 3.3: *traceroute* para o endereço `a.dns.usp.br`

```
user@localhost - ~$ traceroute -I a.dns.usp.br

traceroute to a.dns.usp.br (200.144.248.208), 30 hops max, 60
   byte packets
 1  _gateway (143.54.85.1)  1.532 ms  1.467 ms  1.671 ms
 2  143.54.3.70 (143.54.3.70)  1.384 ms  1.386 ms  1.367 ms
 3  lsv-routcs.ufrgs.br (143.54.0.137)  1.651 ms  1.642 ms
    1.733 ms
 4  143.54.0.193 (143.54.0.193)  1.295 ms  1.310 ms  1.303 ms
 5  143.54.0.246 (143.54.0.246)  1.239 ms  1.218 ms  1.173 ms
 6  lsf-out.ufrgs.br (143.54.0.254)  1.500 ms  1.395 ms  1.375
    ms
 7  ufrgs-ve-40-mlxe8.tche.br (200.19.240.13)  1.426 ms  1.418
    ms  1.629 ms
 8  mlxe4.tche.br (200.19.246.6)  1.374 ms  1.445 ms  1.439 ms
 9  as1916.portoalegre.rs.ix.br (200.219.143.3)  1.308 ms  1.295
     ms  1.289 ms
10  sc-rs-oi.bkb.rnp.br (200.143.252.58)  9.273 ms  9.254 ms
   9.245 ms
11  sp-sc-oi.bkb.rnp.br (200.143.252.65)  21.487 ms  21.496 ms
   20.655 ms
12  sp-usp.bkb.rnp.br (200.143.255.114)  21.805 ms  21.810 ms
   21.802 ms
13  143.107.151.62 (143.107.151.62)  20.288 ms  20.295 ms
   20.559 ms
14  a.dns.usp.br (200.144.248.208)  20.215 ms  20.098 ms  20.089
    ms
```

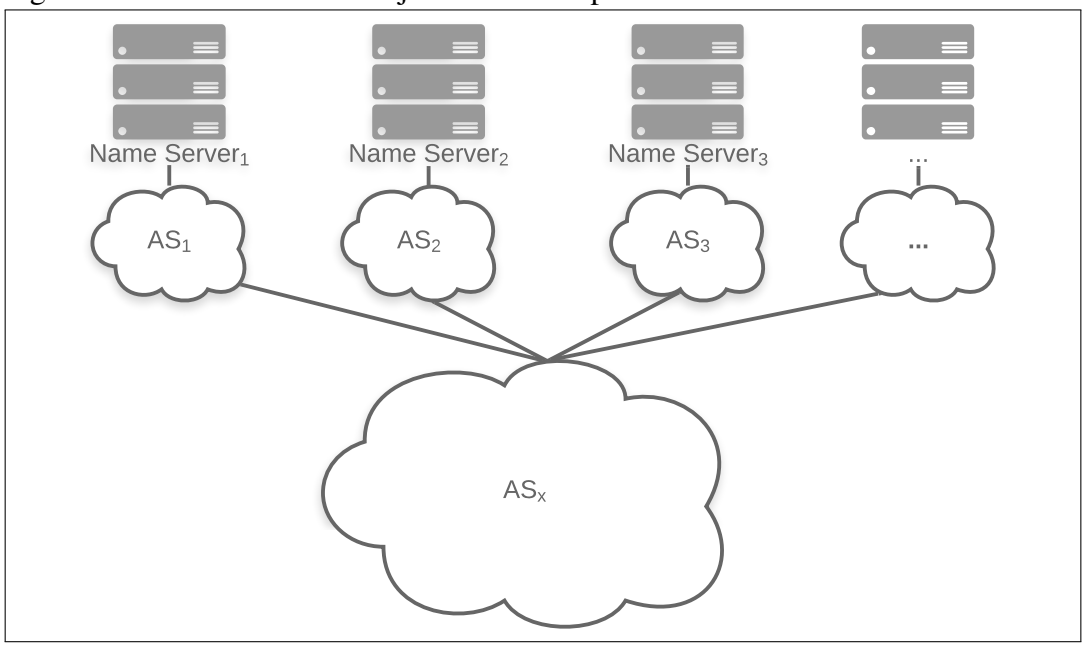
A ferramenta *traceroute* é amplamente utilizada para a realização de diagnósticos em infraestruturas de rede. No entanto, ela não possui suporte ao paralelismo necessário para realizar medições, de forma simultânea, em um grande grupo de domínios de maneira confiável. Os detalhes deste problema, e a consequente necessidade de implementação de uma customização sobre a ferramenta original são descritos no capítulo 4.

3.2 Metodologia Proposta

A presente proposta baseia-se na realização de medições ativas a servidores DNS autoritativos, com base na lista *Alexa's Top 1 Million*, que representa o conjunto de 1.000.000 de *web sites* mais acessados da internet. Essa escolha foi motivada pelo fato de que as zonas de DNS de primeiro nível possuem, em sua maioria, um grande número de domínios estacionados (*parked domains*) (VISSERS; JOOSEN; NIKIFORAKIS, 2015). Tais domínios normalmente compartilham, em grande volume, um número pequeno de servidores DNS autoritativos. Este alto volume de compartilhamento pode distorcer o real risco do compartilhamento de infraestrutura, tendo em vista que um ataque a um servidor responsável por domínios estacionados tem potencial para indisponibilizar uma série de domínios. Contudo, o impacto percebido do ataque é baixo, pois tais domínios possuem um baixo volume de acesso. Esta distorção não ocorre quando restringimos o conjunto de sites analisados, de forma a considerar apenas *websites* que possuam um volume representativo de acesso por usuários. Por este motivo, a lista *Alexa's Top 1 Million* foi escolhida como base de domínios a ser analisada.

Para cada domínio na lista *Alexa's Top 1 Million*, inicialmente, utiliza-se a ferramenta *dig* para descobrir os servidores DNS autoritativos à cada domínio. De forma geral, cada domínio possui, normalmente, de um a quatro servidores autoritativos distintos. No entanto, como alguns domínios compartilham os mesmos servidores autoritativos, o número total de servidores autoritativos distintos obtidos é de aproximadamente 280.000. Em seguida, é executada, para cada servidor autoritativo, a ferramenta *traceroute* a partir de um servidor de coleta. Com essa execução, é possível obter os endereços de cada salto presente na rota entre o cliente e o servidor DNS autoritativo. Quando um conjunto de servidores distintos, responsáveis por domínios de diferentes *websites*, estão hospedados sobre a infraestrutura de um mesmo provedor, requisições enviadas para estes servidores irão compartilhar um ponto em comum - o salto de rede logo antes de chegar ao seu destino final - doravante denominado *Hop-Before-The-Last* (HBTL). Caso duas requisições para servidores diferentes sejam enviadas através de uma rota cujos HBTL estejam sob o mesmo Sistema Autônomo, é provável que ambos sejam hospedados pelo mesmo provedor DNS e que, consequentemente, ambos estejam compartilhando a mesma infraestrutura. Tal compartilhamento é ilustrado na figura 3.2.

Figura 3.2: Servidores DNS cujos HBTL compartilham o mesmo Sistema Autônomo

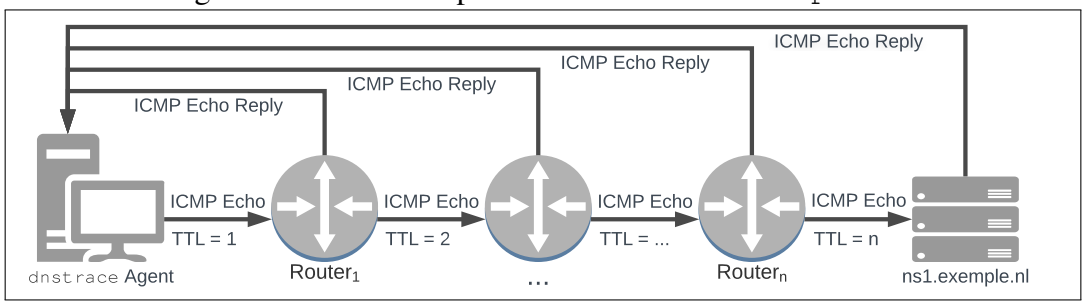


Fonte: Autor

A metodologia proposta é ilustrada pela figura 3.3. Inicialmente, pacotes ICMP do tipo *Echo Request* são enviados aos servidores DNS autoritativos a um dado domínio. Com base nestes pacotes, é possível traçar a rota percorrida até o servidor DNS. Desta informação, armazenamos apenas os dados do último salto, bem como os do HBTL - estes são os pontos mais prováveis de agregação de infraestrutura no ecossistema DNS. Em seguida, obtemos os endereços IP associados a estes saltos. Para cada um deles, é utilizada uma tabela BGP pública para obter o Sistema Autônomo ao qual o endereço pertence, bem como a empresa responsável por ele. Este passo é repetido para o endereço de destino e para o HBTL.

Finalmente, tendo obtido e processado as respostas dos saltos relativos à rota para o servidor DNS autoritativo, estas informações são armazenadas em uma única entrada de banco de dados, para análise futura. Ao executar este processo repetidamente, é possível consolidar milhões de entradas no banco de dados, como forma de identificar possíveis agregações de infraestrutura, em diferentes níveis, bem como analisar as mudanças sofridas pelo ecossistema DNS ao longo do tempo. Durante o estudo de caso, esse processo foi executado mensalmente, de Janeiro de 2018 até Maio de 2018, resultando num conjunto de dados bruto de aproximadamente 20GB.

Figura 3.3: *traceroute* para o domínio `ns1.example.nl`



Fonte: Autor

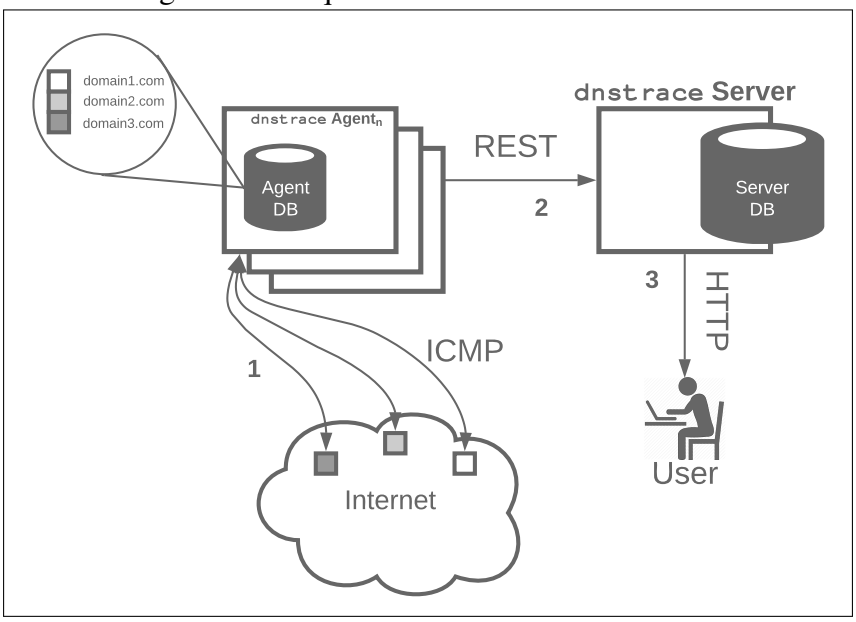
4 *DNSTRACE*

Para suportar a metodologia proposta, bem como para permitir a realização do estudo de caso, a ferramenta *dnstrace* foi desenvolvida. Ela permite coletar informações relacionadas aos serviços DNS, com o objetivo de expor o nível de centralização da infraestrutura DNS. Com ela pesquisadores, operadores de rede e usuários em geral podem visualizar a concentração do DNS numa interface web de fácil utilização. Nesse capítulo, são abordados os detalhes da arquitetura técnica, implementação e funcionamento da ferramenta *dnstrace*.

4.1 Arquitetura Proposta e Tecnologias Utilizadas

De forma a permitir uma melhor administração da ferramenta e facilitar a distribuição de agentes em diversos pontos de coleta, a ferramenta foi desenvolvida com base em uma arquitetura distribuída. A figura 4.1 ilustra a arquitetura da ferramenta. No lado esquerdo, um conjunto de agentes efetua as coletas, a partir de pontos distintos, com base na lista de servidores autoritativos aos domínios presentes na lista *Alexa's Top 1 Million* (1). Após essa coleta, a informação é processada pelo agente e o resultado é enviado ao servidor, que, por sua vez, armazena a informação coletada em um banco de dados, atualizando o status de cada execução (2). O servidor também expõe uma interface Web que pode ser acessada pelo usuário para visualizar os resultados das consultas (3). Os detalhes de implementação de cada uma destas camadas são descritos nas seções abaixo.

Figura 4.1: Arquitetura da ferramenta *dnstrace*



Fonte: Autor

4.1.1 *dnstrace: Agente*

O agente *dnstrace* contém o cerne da lógica por trás do funcionamento da ferramenta. Ele é responsável por obter os dados de servidores DNS autoritativos a um domínio, por realizar o rastreamento da rota até estes servidores, bem como por mapear os endereços de IP obtidos a Sistemas Autônomos. Todas estas tarefas são consideradas I/O-intensivas. Tendo em vista esta característica, a implementação do agente precisa explorar com eficiência técnicas de paralelismo, de forma a minimizar o tempo total necessário para realização das coletas.

A implementação do agente foi realizada integralmente na linguagem de programação Java (JDK 8). Para a organização do projeto e gerência de dependências, foi utilizado o gerente de projetos Maven, versão 3.5.2. O projeto foi organizado levando em conta o padrão de arquitetura de software MVC (*Model View Controller*). Esta organização foi abstraída pelo *framework Spring Boot*, versão 2.1.0. Toda a comunicação entre o agente e o servidor é realizada através de chamadas HTTP REST com dados no formato JSON.

Cada agente possui um arquivo de configuração, onde é possível parametrizar, dentre outros, o identificador do agente. Este parâmetro é importante para permitir a identificação do agente pelo servidor, bem como para permitir a associação de agentes a

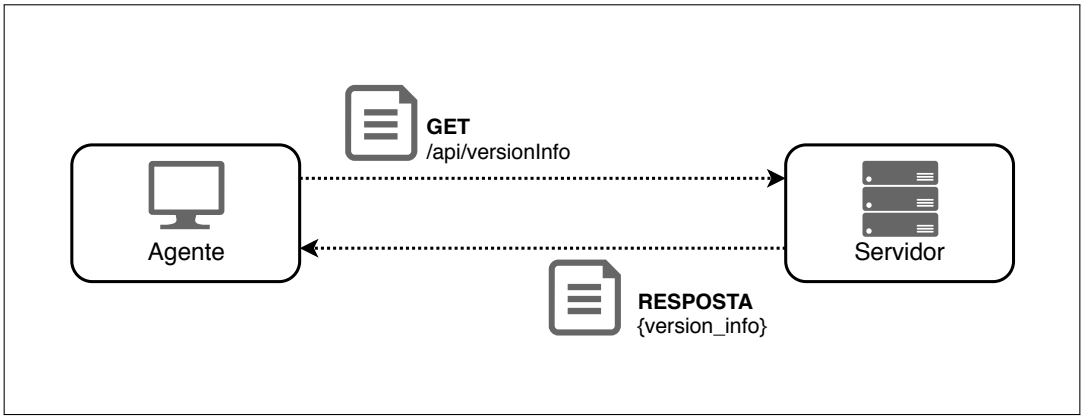
locais físicos distintos (o que é importante na análise dos dados gerados).

Ao ser iniciado, o agente carrega em memória e inicializa as duas bases de dados que são necessárias durante a sua execução:

1. Lista *Alexa's Top 1 Million*: A lista é carregada com base em um arquivo CSV disponibilizado publicamente (Alexa, 2018).
2. Tabela BGP: Possuir conhecimento da tabela BGP é necessário, pois, com base nos prefixos anunciados, é possível determinar a qual Sistema Autônomo pertence o bloco de IPs ao qual um determinado endereço IP está associado (RIPE Network Coordination Centre, 2018).

Após essa inicialização, o agente envia uma requisição ao servidor informando o seu identificador. Com base nele, o servidor consulta a sua base de dados para determinar se já existe alguma coleta em execução para este agente. Em caso positivo, o servidor retorna ao agente a lista de domínios que já foi processada durante esta execução. Tal alinhamento permite a retomada de uma execução que possa ter sido interrompida por algum problema (queda do servidor, queda do agente, problemas de comunicação, dentre outros). Caso nenhuma execução pendente seja encontrada, o servidor registra o início de uma nova execução, retornando ao agente o comando para iniciar uma nova coleta. Essa comunicação é ilustrada pela figura 4.2.

Figura 4.2: Chamada para a rota `/api/versionInfo`

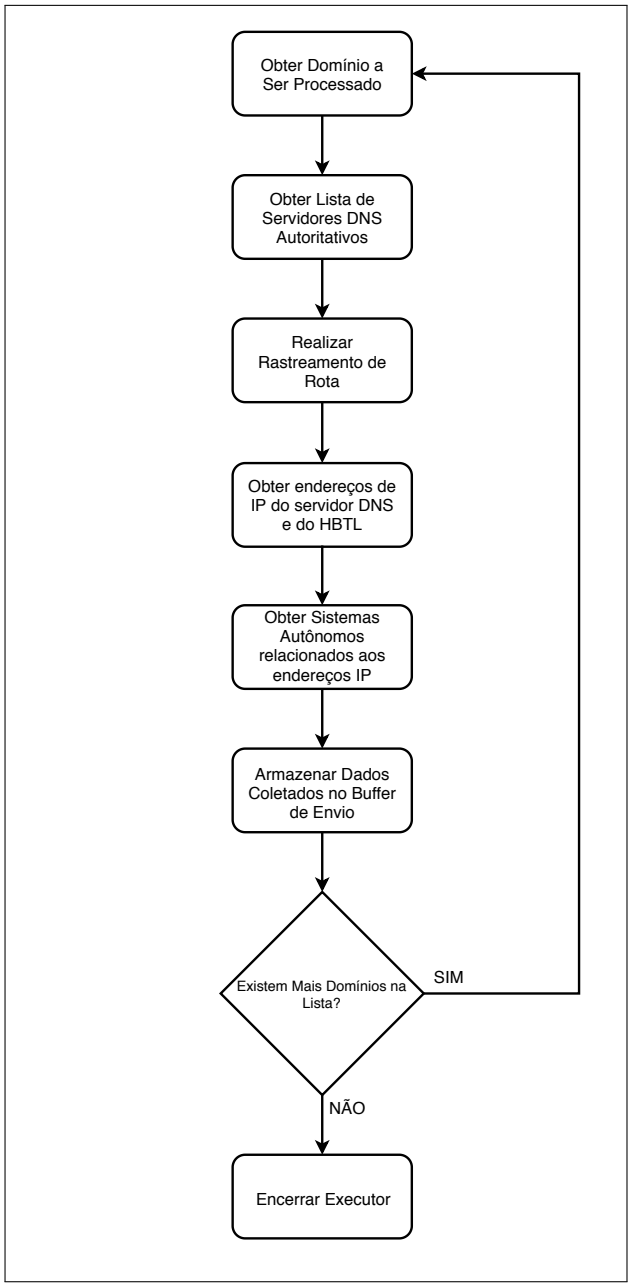


Fonte: Autor

Quando uma nova coleta é iniciada, é criado um novo *thread pool* com instâncias de executores. Tais executores têm como tarefa realizar a coleta de informações para um dado domínio. O tamanho deste *thread pool* é parametrizável, o que permite dimensionar o agente coletor de acordo com a capacidade do servidor onde ele está alocado. Caso o parâmetro não seja informado, ele é inicializado com o valor padrão 150. Ou seja,

150 domínios distintos serão processados simultaneamente, por padrão. Cada um destes executores executa o algoritmo de coleta para um domínio de forma independente.

Figura 4.3: Algoritmo executado pelos coletores no agente *dnstrace*

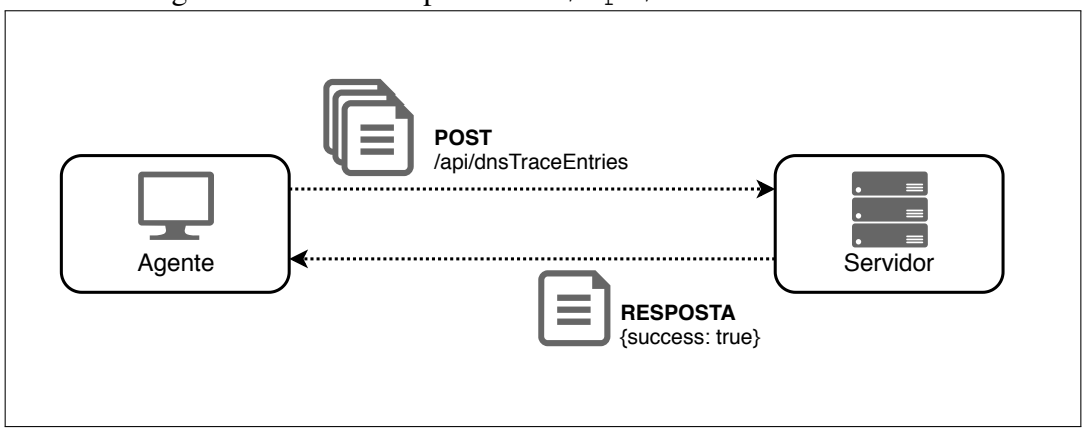


Fonte: Autor

Inicialmente, o coletor obtém um nome de domínio a ser processado com base na lista *Alexa's Top 1 Million*, carregada durante a sua inicialização. Ao obter o domínio a ser processado, o mesmo é removido da lista de forma a não ser processado em duplicidade pelos demais coletores. Isso é feito em uma transação atômica. Após possuir o nome do domínio, o coletor executa um comando *dig* para obter a relação de servidores DNS autoritativos a ele. Em seguida, para cada um dos servidores DNS encontrados, é

realizado o rastreamento da rota de rede até ele, utilizado uma versão customizada do comando *traceroute*. Dessa rota são extraídos os endereços IP de dois pontos de interesse: o servidor DNS alvo e o salto de rede imediatamente anterior ao servidor DNS alvo (*Hop-Before-The-Last*). Para ambos endereços, é utilizada a tabela BGP para mapear os Sistemas Autônomos aos quais cada um deles pertence. Todas estas informações são armazenadas em um *buffer*, que será enviado ao servidor *dnstrace*, após o mesmo atingir um tamanho pré determinado. Este *buffer* é utilizado como forma de minimizar o volume de chamadas entre o cliente e o servidor, aglomerando uma certa quantidade de registros para que todos sejam transmitidos uma única vez.

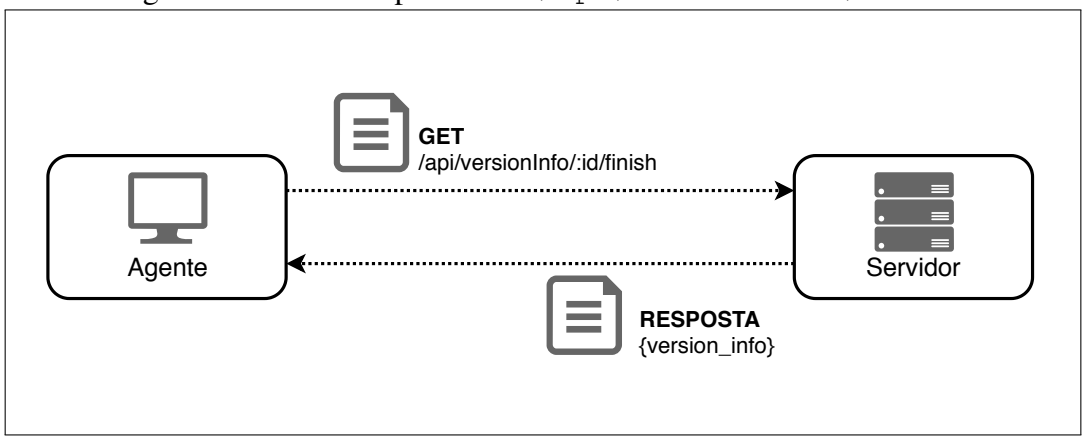
Figura 4.4: Chamada para a rota `/api/dnsTraceEntries`



Fonte: Autor

Os dados coletados são, então, enviados ao servidor através de uma chamada REST, ilustrada na figura 4.4. Este processo é repetido pelo executor até que todos os domínios tenham sido processados. Após concluído o processamento de todos os domínios, os executores são finalizados e o agente envia uma requisição ao servidor, informado a conclusão bem sucedida da operação de coleta. Tal requisição é ilustrada pela figura 4.5.

Figura 4.5: Chamada para a rota `/api/versionInfo/finish`

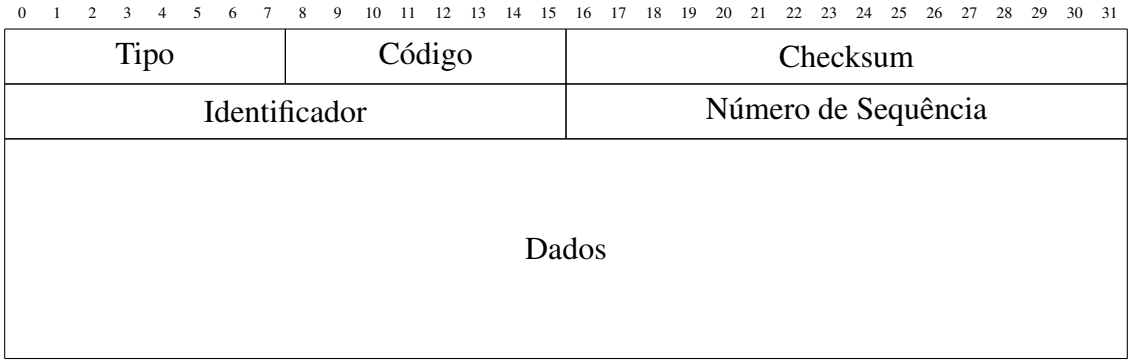


Fonte: Autor

4.1.2 Ferramenta *traceroute* Customizada

A ferramenta *traceroute* foi originalmente desenvolvida com o objetivo de permitir a análise de rotas por administradores de rede, auxiliando na resolução de problemas. O seu princípio de funcionamento baseia-se no envio de pacotes ICMP do tipo *Echo Request*.

Figura 4.6: Esquema de um pacote ICMP *Echo Request* ou *Echo Reply*



Fonte: (POSTEL, 1981a)

A ferramenta, no entanto, não foi desenvolvida tendo em vista a sua aplicação em problemas que necessitem execuções simultâneas, dentro de um mesmo processo. Além disso, devido à forma como foi implementada, há a possibilidade de colisão de identificadores de pacotes em sistemas operacionais de 64 *bits*, o que acarreta na má gerência das respostas recebidas pelo sistema operacional, gerando erros na interpretação dos dados fornecidos pela ferramenta. O trecho de código 4.1 foi retirado do código-fonte da ferramenta *traceroute* implementada no sistema operacional *FreeBSD* (MIT, 2018).

Código 4.1: Trecho de código da ferramenta *traceroute*

```
1  outip->ip_dst = to->sin_addr;
2  outip->ip_hl = (outp - (u_char *)outip) >> 2;
3
4  ident = (getpid() & 0xffff) | 0x8000;
5
6  if (pe == NULL) {
7    Fprintf(stderr, "%s: unknown protocol %s\n", prog, cp);
8    exit(1);
9  }
```

Na linha 4, é possível observar a operação realizada pela ferramenta para atribuir o campo de identificação aos pacotes ICMP a serem enviados. Ao considerar apenas os *bits* menos significativos do identificador do processo (através da máscara `0xffff`), a implementação abre brechas para a ocorrência de colisões de identificadores, em casos específicos, como no simulado pelo código 4.2. Além disso, a ocorrência de colisões é evidente em casos onde várias instâncias da ferramenta são executadas em paralelo por um mesmo processo.

Código 4.2: Simulação de colisão de identificadores

```
1  #include <sys/types.h>
2  #include <unistd.h>
3
4  int main()
5  {
6      pid_t pid1 = 5;
7      pid_t pid2 = 65541;
8
9      pid_t ident1 = (pid1 & 0xffff) | 0x8000;
10     pid_t ident2 = (pid2 & 0xffff) | 0x8000;
11
12     printf("Packet ID1: %d\nPacket ID2: %d", ident1, ident2);
13
14     return 0;
15 }
```

O código 4.2, escrito na linguagem *C*, simula o cálculo de identificadores realizado pela ferramenta *traceroute* em um sistema operacional de 64 *bits*, considerando um cenário hipotético onde a ferramenta esteja sendo executada por dois processos simultaneamente. Neste cenário, tais processos possuem os PIDs 5 e 65541. Na simulação, os

identificadores gerados pela ferramenta *traceroute* são iguais, o que evidencia a ocorrência de colisão.

Código 4.3: Resultado da execução do Código 4.2

```
user@localhost - ~$ ./simulador_colisao

Packet ID1: 32773
Packet ID2: 32773

...Program finished with exit code 0
Press ENTER to exit console.
```

De forma a contornar este problema, foi necessário implementar uma versão customizada da ferramenta *traceroute*, que não tenha a mesma limitação relacionada a execuções simultâneas. Como a linguagem de programação Java não possui suporte nativo à manipulação em baixo nível de *sockets*, devido a particularidades de cada sistema operacional, foi utilizada a biblioteca JNI de código aberto *RockSaw* (SAVARESE, 2018). Esta biblioteca fornece uma interface de baixo nível para os *sockets* nativos do sistema operacional, que é necessária para o envio de pacotes ICMP. Com o uso da biblioteca foi possível reproduzir a mesma funcionalidade da ferramenta *traceroute*. Para isso, foi implementada a classe *RawTraceRoute*, que, utilizando a interface para *sockets* nativos fornecida pela biblioteca, permitiu reproduzir a funcionalidade do *traceroute* original, adicionando suporte a execuções paralelas. Ao instanciar a classe, é possível informar o identificador a ser utilizado pelo pacote, conforme mostra o código 4.4. Na implementação do agente da ferramenta *dnstrace*, cada *thread* é criada com base em um identificador incremental único, que é passado como identificador para o pacote ICMP gerado, eliminando o problema de colisão de identificadores.

Código 4.4: Trecho de código de inicialização da classe *RawTraceRoute*

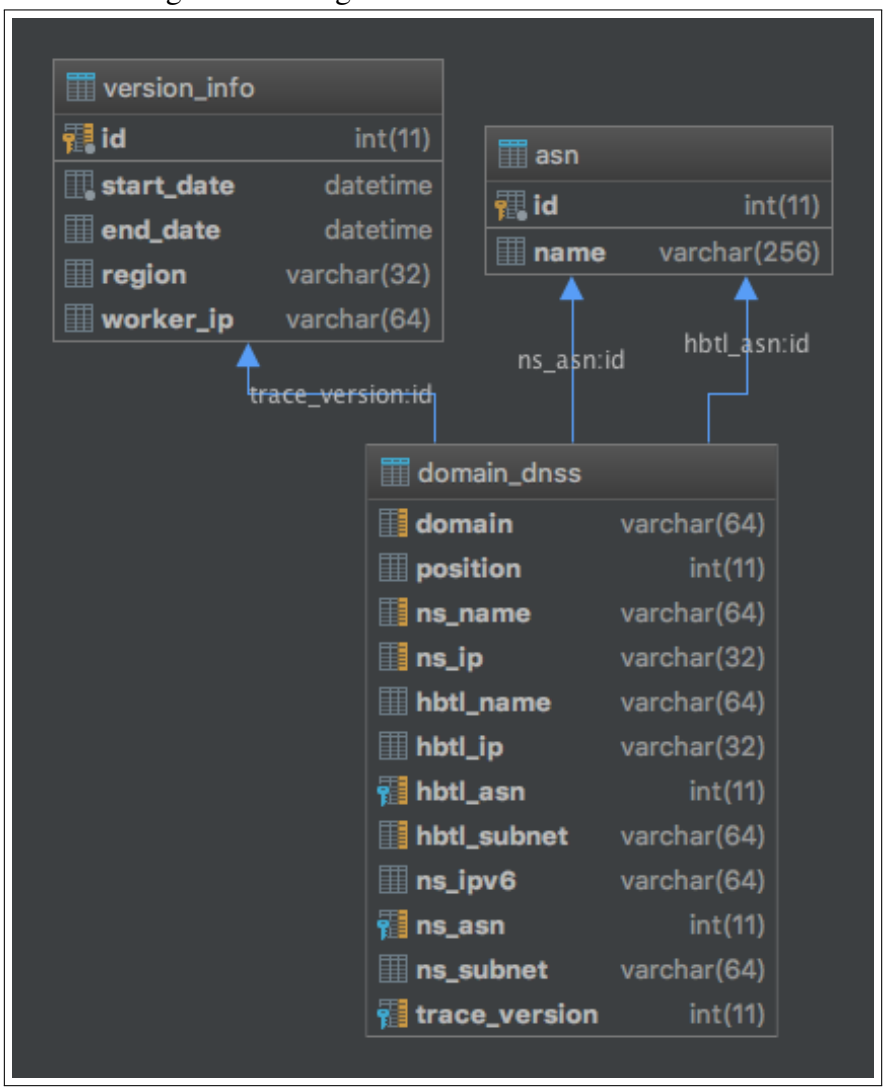
```
public RawTraceRoute(int id, int protocolFamily, int protocol) {
      this.sequence = 0;
      this.identifier = id;
      this.protocolFamily = protocolFamily;
      this.protocol = protocol;
}
```

4.1.3 *dnstrace: Servidor*

Assim como no agente, a implementação do servidor foi realizada integralmente na linguagem de programação Java (JDK 8). Para a organização do projeto e gerência de dependências, também foi utilizado o gerente de projetos Maven, versão 3.5.2. O projeto foi organizado levando em conta o padrão de arquitetura de software MVC (*Model View Controller*). Esta organização foi abstraída pelo *framework Spring Boot*, versão 2.1.0. Para armazenar os dados gerados pelos coletores, foi utilizado o banco de dados relacional *MySQL*, versão 5.7.25. Para a realização do mapeamento objeto-relacional (ou ORM, do inglês: *Object-relational mapping*), foi utilizada a ferramenta Hibernate, versão 5.3.1.

O servidor da ferramenta *dnstrace* expõe diferentes rotas REST. Tais rotas são utilizadas pelos agentes de coleta para obter e enviar informações relacionadas à sua execução. Este conjunto de rotas também é utilizado pela interface WEB de forma a obter os dados requisitados pelo usuário para visualização. O conjunto de rotas exposto pelo servidor é detalhado na tabela 4.1. Todos os dados gerados durante as coletas são armazenados no banco de dados, cujo diagrama é ilustrado na figura 4.7.

Figura 4.7: Diagrama Entidade-Relacionamento



Fonte: Autor

Tabela 4.1: Tabela de rotas do servidor *dnstrace*

Método	URI	Descrição
GET	/api/versionInfo	Retorna os dados de uma execução de coleta pendente em um determinado agente. Caso nenhuma execução pendente seja encontrada, é gerado um novo identificador de execução. Os dados enviados durante esta chamada estão detalhados na tabela 4.2.
POST	/api/versionInfo/:id/finish	Encerra uma determinada execução de coleta.
GET	/api/allAvailableRuns	Lista os detalhes de todas as execuções pendentes.
GET	/api/dnsTraceEntry	Obtém uma entrada da coleta de informações sobre um servidor DNS com base no seu identificador.
POST	/api/dnsTraceEntries	Recebe uma lista de entradas de coleta e salva-as no banco de dados, atualizando o status da execução. Esta é a rota chamada pelos agentes da ferramenta para enviar um lote de resultados de coleta. Os dados enviados durante esta chamada estão detalhados na tabela 4.3.
GET	/api/processedDomains	Retorna a lista de domínios já processados para uma determinada execução de coleta.
GET	/api/statistics	Retorna as estatísticas de execução de coletas já realizadas.
GET	/api/resultData	Retorna os dados de resultado de uma determinada coleta, seguindo uma determinada agregação.

Fonte: Autor

Para cada execução de coleta, é armazenado no banco de dados um registro na tabela `version_info`, cujo mapeamento objeto-relacional, dá-se pela tabela 4.2.

Tabela 4.2: Modelo de Dados - Instância de Execução de Coleta

Nome	Tipo	Descrição
id	Inteiro	Identificador da execução.
startDate	*DateTime*	Data e Hora do início da execução.
endDate	*DateTime*	Data e Hora do término da execução. Este campo recebe o valor nulo caso a coleta ainda não tenha sido finalizada.
region	Texto	Identificador da região de coleta (utilizado como identificador do agente).
workerIp	Texto	Endereço IP do agente responsável pela coleta.

Fonte: Autor

Durante o processamento da coleta para um dado domínio, um novo registro no banco de dados é gerado para cada servidor DNS autoritativo a ele. Este registro é armazenado na tabela `domain_dnss`, cujo mapeamento objeto-relacional dá-se pela tabela 4.3.

Tabela 4.3: Modelo de Dados - Dados Coletados por Servidor DNS

Nome	Tipo	Descrição
traceVersion	Inteiro	Identificador da execução ao qual o registro está vinculado.
domain	Texto	Nome do Domínio ao qual o Servidor DNS está associado.
position	Inteiro	Posição do domínio na lista *Alexa's Top 1 Million*.
nsName	Texto	Nome do Servidor DNS.
nsIp	Texto	Endereço IP do Servidor DNS.
nsIpv6	Texto	Endereço IPv6 do Servidor DNS.
nsAsn	Inteiro	Número do Sistema Autônomo do Servidor DNS.
nsSubnet	Texto	Máscara de Subrede do Servidor DNS.
hbtlName	Texto	Nome do *Hop-Before-The-Last*.
hbtlIp	Texto	Endereço IP do *Hop-Before-The-Last*.
hbtlAsn	Inteiro	Número do Sistema Autônomo do *Hop-Before-The-Last*.
hbtlSubnet	Texto	Máscara de Subrede do *Hop-Before-The-Last*.

Fonte: Autor

Durante a geração de resultados, torna-se importante identificar, através do nome, os Sistemas Autônomos associados a um determinado registro. Esta identificação é realizada pela tabela `asn`, cujo mapeamento objeto-relacional dá-se pela tabela 4.3. A tabela foi carregada inicialmente com os dados de Sistemas Autônomos mantido pela ARIN, agência responsável pelo registro de Sistemas Autônomos na América do Norte (ARIN, 2018).

Tabela 4.4: Modelo de Dados - Sistema Autônomo

Nome	Tipo	Descrição
id	Inteiro	Identificador numérico do Sistema Autônomo (ASN).
name	Texto	Nome do Sistema Autônomo.

Fonte: Autor

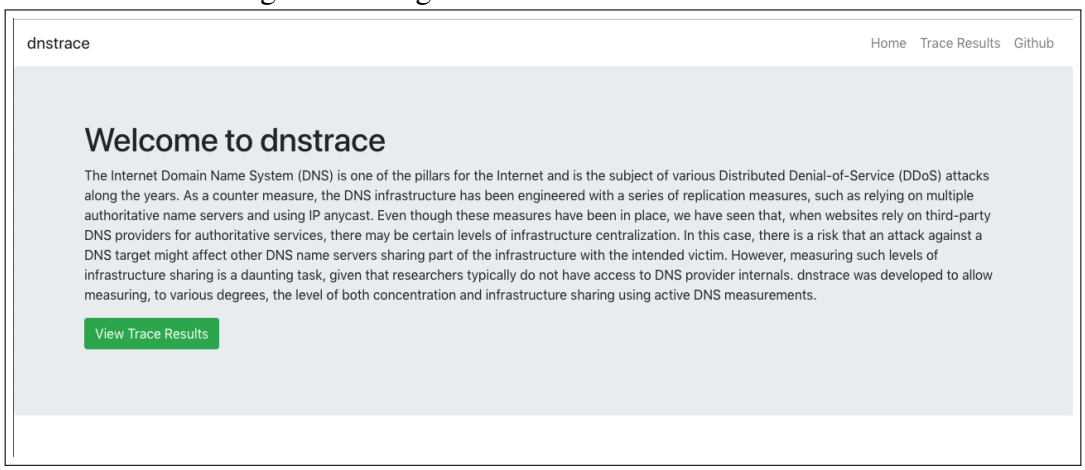
4.1.4 *dnstrace: Interface WEB*

Com o objetivo de permitir fácil acesso aos resultados de coleta obtidos pela ferramenta *dnstrace*, foi desenvolvida uma interface WEB, que comunica-se com o servidor para obter os dados a serem visualizados. A interface foi implementada em JavaScript, utilizando o *framework React*, versão 16.6. Para a criação das janelas, foi utilizado o *framework Bootstrap*, versão 4. Para a organização do projeto e gerência de dependências, foi utilizado o gerente de projetos Maven, versão 3.5.2. O projeto foi organizado levando em conta o padrão de arquitetura de software MVC (*Model View Controller*). Esta organização foi abstraída pelo *framework Spring Boot*, versão 2.1.0. Além disso, foi utilizado o servidor WEB Tomcat, versão 8, incluído no *Spring Boot*.

A página inicial da ferramenta *dnstrace* contém uma introdução ao trabalho e à ferramenta desenvolvida. Através dela, é possível acessar os resultados bem como visualizar o código fonte da ferramenta no *GitHub*[1].

[1] <https://github.com/ComputerNetworks-UFRGS/dnstrace>

Figura 4.8: Página inicial da ferramenta *dnstrace*



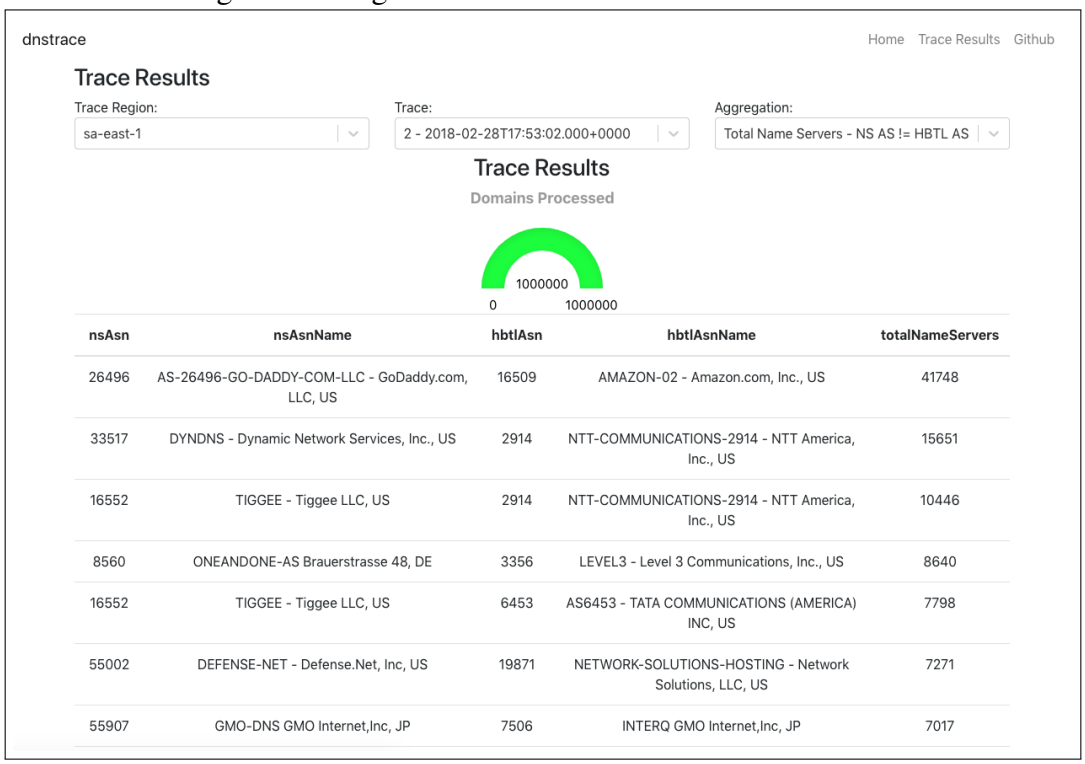
Fonte: Autor

Para acessar a página de resultados, o usuário deve clicar no botão *View Trace Results*. Em seguida, será apresentada uma tela onde o usuário deve escolher as seguintes opções:

1. Trace Region: A região a partir da qual foram realizadas as coletas. Este é o identificador do agente responsável pela coleta.
2. Trace: A coleta em si. As coletas estão ordenadas pelo horário de início da sua execução.
3. Aggregation: A agregação para a qual os dados devem ser processados e exibidos.

Com base nessas escolhas, é enviada uma solicitação ao servidor para que o mesmo busque os dados no banco, realize o processamento da agregação e retorne os dados à interface. É apresentada uma tabela com os resultados, bem como um indicador de quantos domínios já foram processados durante a execução da coleta escolhida.

Figura 4.9: Página de resultados da ferramenta *dnstrace*



nsAsn	nsAsnName	hbtlAsn	hbtlAsnName	totalNameServers
26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US	16509	AMAZON-02 - Amazon.com, Inc., US	41748
33517	DYNDNS - Dynamic Network Services, Inc., US	2914	NTT-COMMUNICATIONS-2914 - NTT America, Inc., US	15651
16552	TIGGEE - Tiggee LLC, US	2914	NTT-COMMUNICATIONS-2914 - NTT America, Inc., US	10446
8560	ONEANDONE-AS Brauerstrasse 48, DE	3356	LEVEL3 - Level 3 Communications, Inc., US	8640
16552	TIGGEE - Tiggee LLC, US	6453	AS6453 - TATA COMMUNICATIONS (AMERICA) INC, US	7798
55002	DEFENSE-NET - Defense.Net, Inc, US	19871	NETWORK-SOLUTIONS-HOSTING - Network Solutions, LLC, US	7271
55907	GMO-DNS GMO Internet,Inc, JP	7506	INTERQ GMO Internet,Inc, JP	7017

Fonte: Autor

5 ESTUDO DE CASO

Nesse capítulo, são apresentados os resultados do estudo de caso realizado com a ferramenta *dnstrace*. No estudo, a ferramenta foi instalada em duas instâncias *Amazon EC2*, na região de São Paulo. Durante a instalação, uma das instâncias foi configurada como Agente *dnstrace*, enquanto a outra foi configurada como Servidor. As duas instâncias possuem a mesma configuração de *hardware* - um único núcleo de CPU e 0.5GB de RAM. Para o banco de dados, foi utilizada uma instância *Amazon Aurora MySQL*, com capacidade para 50GB de dados. Como entrada, foi utilizada a lista *Alexa's Top 1 Million*, contendo o nome do 1 milhão de domínios mais acessados na Internet (Alexa, 2018).

5.1 Conjuntos de Dados

A metodologia foi executada diversas vezes, resultando num conjunto de dados com milhões de registros de coleta. Para cada execução, o agente *dnstrace* coletou dados de cada salto de rede presente na rota para cada servidor DNS autoritativo aos domínios da lista. Nesse estudo, somente as informações do último salto de rede, bem como o HBTL foram armazenadas, além de dados adicionais de endereços IP (que não serão diretamente utilizados nesse estudo, porém poderão ser úteis em trabalhos futuros). A tabela **??** apresenta o resumo dos dados coletados ao longo de cinco meses de observações, executados a partir do servidor de coleta em São Paulo. Observou-se que, ao longo do período observado, o número de servidores DNS autoritativos distintos, bem como o número de AS responsáveis por servidores DNS e seus respectivos HBTL se mantiveram estáveis. Além disso, é possível perceber que o número de servidores DNS autoritativos distintos é muito menor que o número de domínios observados. Isso indica que muitos domínios compartilham os mesmos servidores autoritativos. De fato, dentre os dados coletados, um único servidor autoritativo destaca-se por ser responsável por 10.000 domínios, pertencendo a um grande provedor de serviços DNS: *DNSPod*. Tal fato, no entanto, não indica necessariamente um problema, pois diversos mecanismos de tolerância a falhas podem estar presentes para combater ataques DDoS. Mesmo assim, ele evidencia a existência de centralização na infraestrutura DNS. Dentre as amostras coletadas, 136.421 dos servidores DNS autoritativos analisados continham Sistemas Autônomos em suas rotas que explicitamente descartaram os pacotes ICMP do tipo *Echo Request*, o que impossibilitou a obtenção de informações sobre o HBTL dos respectivos servidores. Por conta disso, tais

servidores foram descartados da análise de agregação de HBTL. Contornar estes empecilhos é um dos tópicos de trabalho futuro desta pesquisa.

Após obter os dados coletados pela ferramenta *dnstrace*, três aspectos foram analisados como forma de identificar a existência de centralização na infraestrutura DNS e do risco de dados colaterais. Em primeiro lugar, foi analisada a concentração de servidores DNS autoritativos por Sistema Autônomo. Em seguida, foi analisada a concentração de Sistemas Autônomos de servidores autoritativos por Sistemas Autônomos dos HBTL. Também foi determinado o número total de servidores DNS autoritativos que compartilham o mesmo HBTL. Estes três aspectos nos permitem medir a quantidade de servidores DNS autoritativos que compartilham a mesma infraestrutura de Sistema Autônomo com outros servidores autoritativos, tanto no nível do último salto, como no nível do HBTL. Finalmente, é analisado se, dentre os principais provedores de serviço DNS, existe uma tendência de aumento desta centralização ao longo do período observado. Cada uma dessas análises é detalhada nas seções a seguir.

5.1.1 Agregação de Servidores DNS Autoritativos por Sistema Autônomo

Nessa primeira observação, é analisada a concentração de servidores DNS autoritativos distintos por Sistema Autônomo. A tabela 5.1 e a figura 5.1 listam os 10 Sistemas Autônomos que agregaram o maior número de servidores DNS autoritativos distintos. Para uma melhor apresentação, cada Sistema Autônomo presente na tabela 5.1 é referenciado por um identificador que o representa na figura 5.1. A tabela também apresenta o nome e o identificador numérico de cada Sistema Autônomo (ASN). Como pode-se observar, a maioria dos Sistemas Autônomos apresentados pertencem a grandes provedores de infraestrutura.

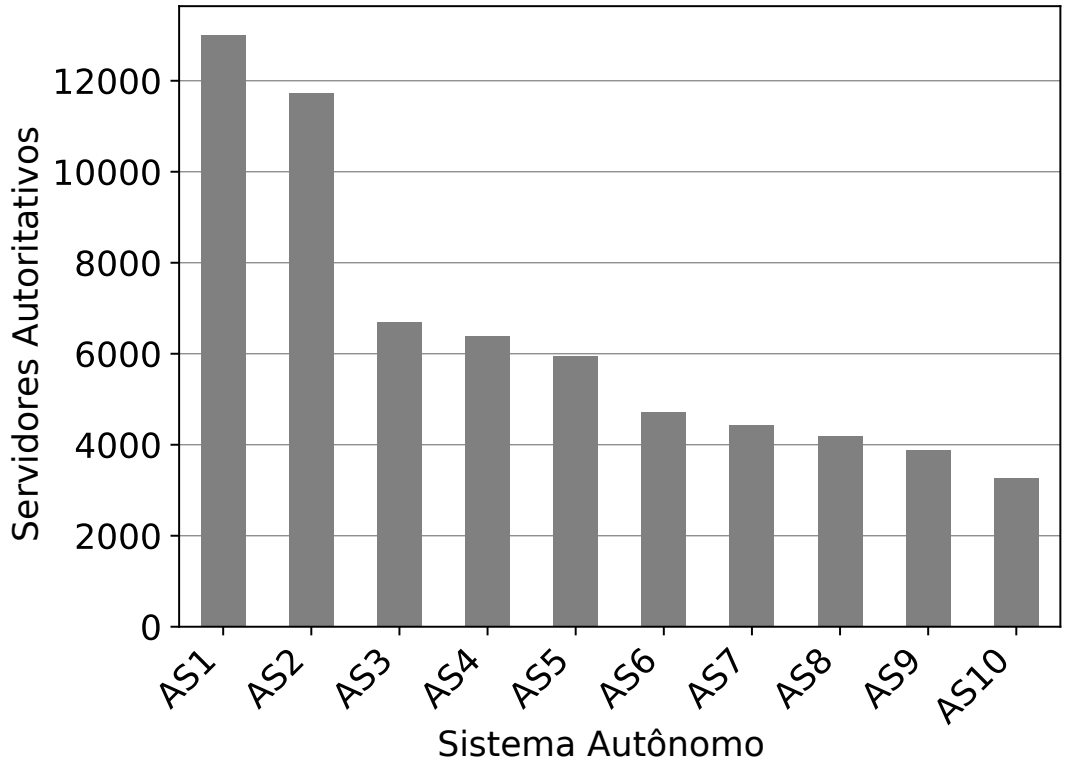
A figura mostra que o provedor "OVH, FR", identificado na tabela 5.1 como *AS1*, é o provedor DNS com o maior número de servidores autoritativos em sua infraestrutura, agregando um total de mais de 12.000 servidores autoritativos distintos, cada um responsável por múltiplos domínios. Isso significa que, no caso de um ataque bem sucedido a esse Sistema Autônomo, mais de 12.000 dos *web sites* mais acessados no mundo ficariam indisponíveis, pois os usuários não conseguiram resolver os seus endereços. Observa-se, também, que o provedor "HETZNER-AS, DE", identificado como *AS2*, mantém um total de 11.000 servidores autoritativos, seguido pelo *AS3* - "UNIFIEDLAYER-AS-1 - Unified Layer, US", que hospeda 6.000 servidores autoritativos em sua infraestrutura. Estes três

Tabela 5.1: Agregação de Servidores DNS Autoritativos por Sistema Autônomo

ID	Sistema Autônomo	Servidores Autoritativos	ASN
AS1	OVH, FR	12.990	16.276
AS2	HETZNER-AS, DE	11.730	24.940
AS3	UNIFIEDLAYER-AS-1 - Unified Layer, US	6.698	46.606
AS4	CLOUDFLARENET - CloudFlare, Inc., US	6.384	13.335
AS5	CYRUSONE - CyrusOne LLC, US	5.955	20.013
AS6	SINGLEHOP-LLC - SingleHop, Inc., US	4.710	32.475
AS7	AMAZON-02 - Amazon.com, Inc., US	4.421	16.509
AS8	TIGGEE - Tiggee LLC, US	4.182	16.552
AS9	LIQUID-WEB-INC - Liquid Web, L.L.C, US	3.890	32.244
AS10	SOFTLAYER - SoftLayer Technologies Inc., US	3.265	36.351

Fonte: Autor

Figura 5.1: Agregação de Servidores DNS Autoritativos por Sistema Autônomo



Fonte: Autor

Sistemas Autônomos, no topo da lista, reúnem um grande risco de danos colaterais, por concentrarem um grande número de servidores autoritativos. Partindo do *AS4* ao *AS10*, pode-se observar uma agregação que varia de 6.000 a 3.000 servidores autoritativos em

cada provedor. Este grau de centralização já foi apontado por pesquisas realizadas no passado (ALLMAN, 2018), que observaram blocos de IP identificando quantos servidores autoritativos distintos pertenciam a um mesmo bloco. Seguindo tais pesquisas, o presente estudo de caso reforça a existência de centralização nos serviços DNS, o que leva a riscos de dano colateral. Num cenário real, é difícil um ataque derrubar a infraestrutura de um provedor deste tamanho. No entanto, é importante lembrar que os ataques DDoS estão tornando-se cada vez mais sofisticados, como no caso da queda da *DynDNS* (HILTON, 2016), o que torna esse aspecto um ponto de atenção.

5.1.2 Agregação de Servidores DNS Autoritativos por HBTL

Além de analisar o grau de compartilhamento de infraestrutura no nível dos Sistemas Autônomos dos servidores DNS autoritativos, também foi analisada a quantidade de servidores autoritativos que compartilham o mesmo HBTL, já que tal ponto tem a possibilidade de tornar-se um ponto único de falha. A tabela 5.2, bem como a figura 5.2 apresentam os 10 Sistemas Autônomos de HBTL que agregaram o maior número de servidores DNS autoritativos. Para uma melhor apresentação, cada Sistema Autônomo presente na tabela 5.2 é referenciado por um identificador que o representa na figura 5.2, como na análise anterior. A tabela também informa o nome do Sistema Autônomo e o seu identificador numérico (ASN). Como na última análise, pode-se observar que a maioria dos Sistemas Autônomos também pertencem a grandes provedores de infraestrutura.

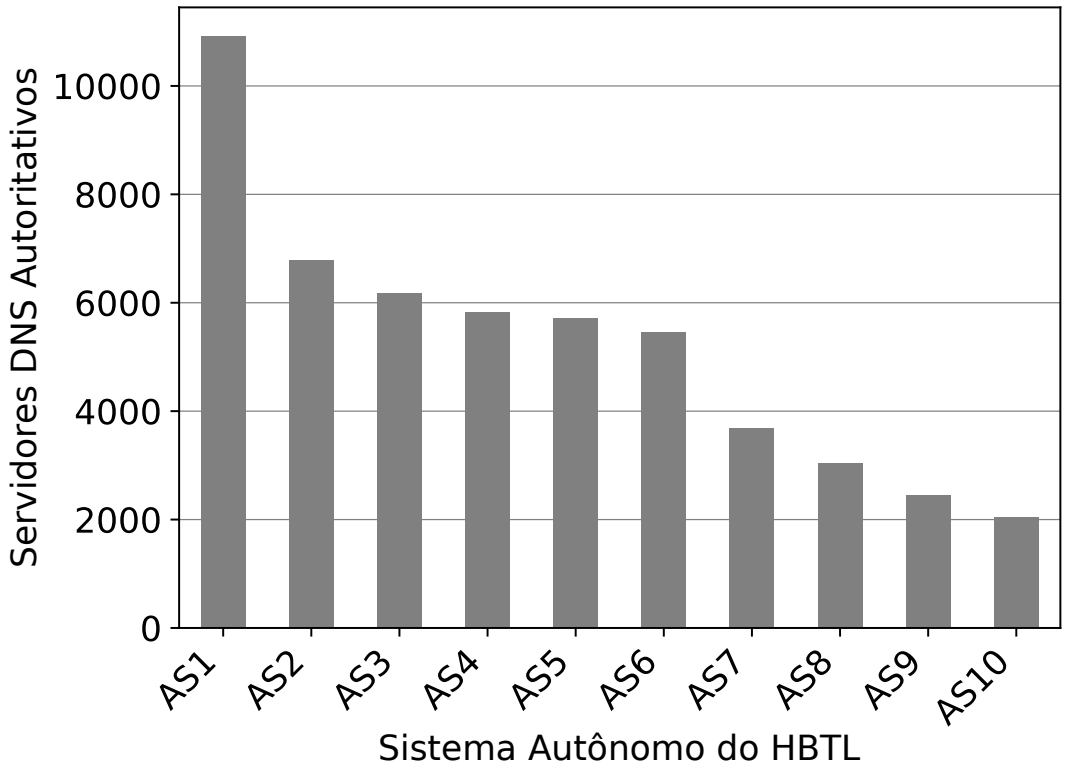
A primeira linha da tabela 5.2, identificada como *AS1*, mostra que quase 11.000 servidores DNS autoritativos compartilham HBTL que encontram-se no Sistema Autônomo "HETZNER-AS, DE". Da mesma forma, a linha identificada como *AS2* mostra que quase 7.000 servidores autoritativos compartilham HBTL sob responsabilidade do Sistema Autônomo "UUNET-SA - MCI Communications Services, Inc. d/b/a Verizon B". Esses números sugerem não só a presença de centralização na infraestrutura DNS no nível de servidores autoritativos, mas também no nível do salto de rede anterior a eles. Adicionalmente, é importante ressaltar que cada um destes servidores autoritativos é responsável por centenas de domínios. Logo. caso algum destes pontos torne-se indisponível em virtude de um ataque, milhares de domínios tornariam-se inacessíveis devido a danos colaterais, o que configura um ponto único de falha.

Tabela 5.2: Agregação de Servidores DNS Autoritativos por HBTL

ID	Sistema Autônomo	Servidores Autoritativos	ASN
AS1	HETZNER-AS, DE	10.904	24.940
AS2	UUNET-SA - MCI Communications Services, Inc. d/b/a Verizon B	6.789	14.551
AS3	UNIFIEDLAYER-AS-1 - Unified Layer, US	6.173	46.606
AS4	CYRUSONE - CyrusOne LLC, US	5.826	20.013
AS5	OVH, FR	5.708	16.276
AS6	LEVEL3 - Level 3 Communications, Inc., US	5.458	3.356
AS7	LIQUID-WEB-INC - Liquid Web, L.L.C, US	3.683	32.244
AS8	SOFTLAYER - SoftLayer Technologies Inc., US	3.043	36.351
AS9	ZAYO-6461 - Zayo Bandwidth Inc, US	2.442	6.461
AS10	SINGLEHOP-LLC - SingleHop, Inc., US	2.037	32.475

Fonte: Autor

Figura 5.2: Agregação de Servidores DNS Autoritativos por HBTL



Fonte: Autor

5.1.3 Agregação de Sistemas Autônomos de servidores DNS autoritativos distintos por Sistemas Autônomos do HBTL

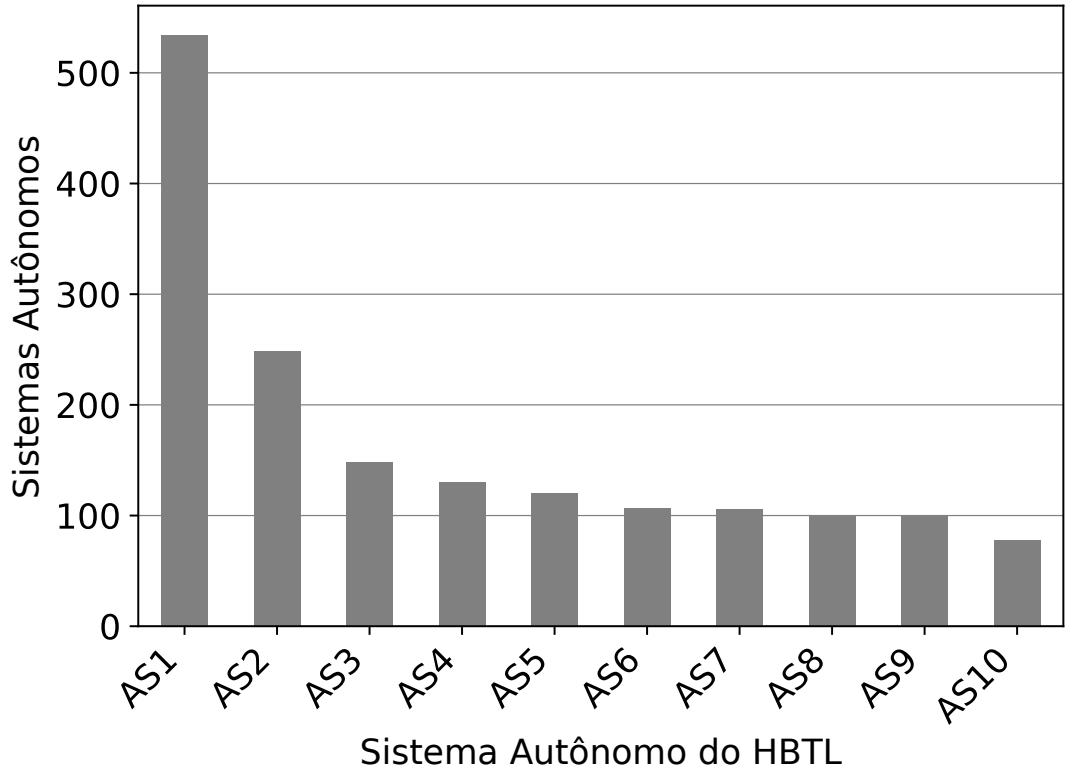
Até então, todas as análises realizadas foram focadas na concentração de servidores DNS autoritativos em realação à cada salto de rede. No entanto, ao observar os Sistemas Autônomos de provedores de serviços de hospedagem, percebe-se que outros serviços podem também ser afetados, além dos servidores DNS autoritativos hospedados por eles. Tendo em vista essa possibilidade, também foi realizada uma análise do número de Sistemas Autônomos distintos que compartilham o mesmo Sistema Autônomo no nível do HBTL. Esta análise tem como objetivo identificar pontos de infraestrutura de rede compartilhados que possam oferecer riscos de dados colaterais para servidores DNS autoritativos. Por exemplo, um serviço totalmente não relacionado pode ser alvo de um ataque e mesmo assim afetar o ecossistema DNS, por causa do compartilhamento de infraestrutura. Novamente, a tabela 5.3 bem como a figura 5.3 relacionam os 10 Sistemas Autônomos de HBTL que concentram o maior número de Sistemas Autônomos distintos como último salto de rede. Para uma melhor apresentação, cada Sistema Autônomo presente na tabela 5.3 é referenciado por um identificador que o representa na figura 5.3. A tabela também informa o nome do Sistema Autônomo e o seu identificador numérico (ASN). Pode-se observar que a maioria dos Sistemas Autônomos pertencem a grandes provedores de infraestrutura e serviços de rede, tais como *Level 3* e *Cogent*.

Tabela 5.3: Agregação de Sistemas Autônomos distintos por Sistemas Autônomos do HBTL

ID	Sistema Autônomo	Total de Sistemas Autônomos	ASN
AS1	LEVEL3 - Level 3 Communications, Inc., US	534	3.356
AS2	COGENT-174 - Cogent Communications, US	248	174
AS3	LVLT-3549 - Level 3 Communications, Inc., US	148	3.549
AS4	HURRICANE - Hurricane Electric, Inc., US	130	6.939
AS5	ROSTELECOM-AS, RU	120	12.389
AS6	TELIANET Telia Carrier, SE	107	1.299
AS7	RETN-AS, UA	106	9.002
AS8	GTT-BACKBONE GTT, DE	99	3.257
AS9	NTT-COMMUNICATIONS-2914 - NTT America, Inc., US	99	2.914
AS10	CENTURYLINK-US-LEGACY-QWEST - Communications Company	78	209

Fonte: Autor

Figura 5.3: Agregação de Sistemas Autônomos distintos em relação aos Sistemas Autônomos do HBTL



Fonte: Autor

Nessa análise, a agregação mais expressiva ocorre no Sistema Autônomo "LEVEL3 - Level 3 Communications, Inc., US", identificado na tabela como *AS1*. A *Level 3* é um dos maiores provedores de infraestrutura de rede do mundo, logo tal resultado é natural. Mesmo assim, o número de Sistemas Autônomos que compartilham a sua infraestrutura é grande, chegando a mais de 500 Sistemas Autônomos distintos. A segunda maior agregação, observada no provedor "COGENT- 174 - Cogent Communications, US- *AS2*, concentra uma agregação de 250 Sistemas Autônomos distintos, menos do que a metade da quantidade observada na *Level 3*. Embora a concentração de Sistemas Autônomos atrás de um salto de rede comum tenha maior relação com a estrutura de roteamento do que diretamente com serviços DNS, tal concentração aumenta o risco de problemas para uma grande quantidade de serviços, caso este venha a sofrer um ataque de larga escala.

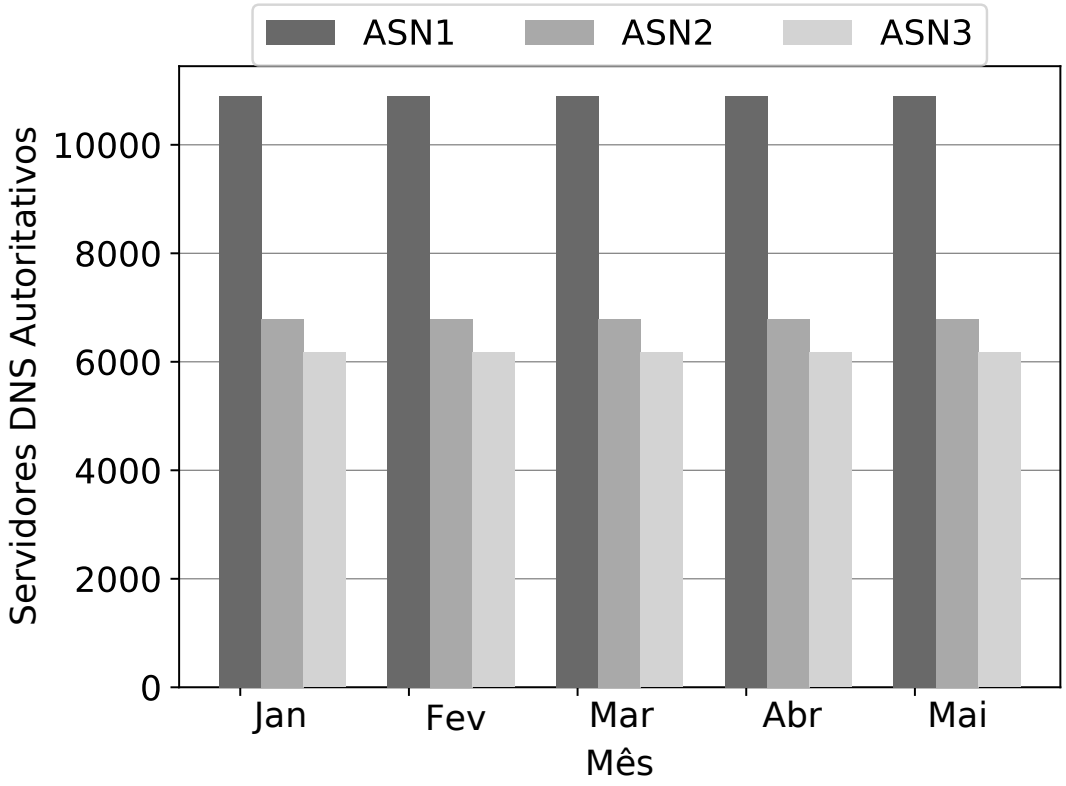
5.1.4 Síntese

A análise detalhada nas seções anteriores mostrou uma presença considerável de compartilhamento de infraestrutura em diferentes níveis do ecossistema DNS. Particularmente, o grau de concentração de servidores DNS autoritativos por HBTL representa alto risco de danos colaterais. É importante ressaltar que muitos operadores de serviços DNS não têm ciência de tal concentração ao escolher um provedor para hospedar seus serviços. Olhar diretamente para o Sistema Autônomo do último salto de rede pode mascarar esse risco, pois muitas empresas alocam endereços de seus próprios blocos IP para seus servidores DNS autoritativos, mesmo hospedando-os por trás da infraestrutura de provedores terceirizados. Nestes casos, o risco de dano colateral também existe.

Finalmente, também foi realizada uma análise temporal na agregação de serviços DNS num período de cinco meses. Esta análise tenta identificar a existência de uma tendência de centralização da infraestrutura DNS durante o período. A figura 5.4 apresenta o grau de agregação nos 3 Sistemas Autônomos que tiveram o maior volume de concentração nas análises anteriores, e a sua evolução ao longo do tempo. Ao observar o gráfico, percebe-se que a centralização de servidores DNS autoritativos à lista de domínios presentes na *Alexa's Top 1 Million* se manteve estável. Isso é consistente com o pressuposto conhecido de que a infraestrutura DNS é estável e robusta. Tal comportamento também pode ser justificado pelo fato de que os provedores observados oferecem um alto grau de confiabilidade, não havendo a necessidade de mudanças frequentes na sua infraestrutura.

No entanto, essa análise não exclui a possibilidade da existência de uma tendência de centralização, quando observado um intervalo de tempo maior.

Figura 5.4: Agregação de Servidores DNS Autoritativos por Sistema Autônomo do HBLT ao longo do tempo



Fonte: Autor

6 CONCLUSÃO

Neste trabalho, foi apresentada a ferramenta *dnstrace*, uma ferramenta que permite medir e visualizar o grau de centralização e de compartilhamento de infraestrutura do DNS da Internet utilizando medições ativas. A ferramenta implementa a metodologia proposta, que baseia-se no uso da ferramenta `traceroute` para rastrear os Sistemas Autônomos associados aos saltos presentes na rota para servidores DNS autoritativos.

Como estudo de caso, a ferramenta *dnstrace* foi utilizada para realizar uma análise focada no grau de centralização de serviços DNS nos Sistemas Autônomos responsáveis pelos *web sites* mais acessados da internet, conforme a lista *Alexa's Top 1 Million*. Foi possível mostrar que, em alguns casos, até 12.000 servidores DNS autoritativos compartilham a mesma infraestrutura de um grande provedor de serviços DNS, podendo sofrer danos colaterais no caso de um ataque, mesmo não sendo o alvo do mesmo. Também foi feita uma análise temporal, utilizando dados coletados ao longo de cinco meses, na tentativa de identificar uma tendência de centralização na infraestrutura DNS. No entanto, nenhuma tendência foi observada durante o período analisado.

Como trabalhos futuros, pode-se considerar a possibilidade de realizar medições utilizando a ferramenta *dnstrace* a partir de diversos pontos de coletas distintos, distribuídos geograficamente ao redor do mundo. Isso irá permitir analisar o nível de influência que a localização física do ponto de coleta exerce sobre a metodologia de observação proposta. Do ponto de vista teórico, também há margem para o desenvolvimento de uma métrica de avaliação de centralização, que possa permitir aos operadores rede uma forma de escolher um provedor de serviços DNS que seja mais adequado às suas necessidades.

REFERÊNCIAS

Alexa. **Alexa Top 1 Million**. 2018. <http://s3.amazonaws.com/alexa-static/top-1m.csv.zip>.

ALLMAN, M. Comments on DNS Robustness. In: **ACM Internet Measurement Conference**. [S.l.: s.n.], 2018. To appear.

AMAZON. **https://www.alexa.com/**. 2018. Disponível em: <https://www.alexa.com/>.

ARIN. **ftp://ftp.arin.net/info/asn.txt**. 2018. Disponível em: <ftp://ftp.arin.net/info/asn.txt>.

BATES, S.; BOWERS, J.; GREENSTEIN, S.; WEINSTOCK, J.; ZITTRAIN, J. **Evidence of Decreasing Internet Entropy: The Lack of Redundancy in DNS Resolution by Major Websites and Services**. [S.l.], 2018.

CONSORTIUM, I. S. **https://linux.die.net/man/1/dig**. 2018. Disponível em: <https://linux.die.net/man/1/dig>.

CONSORTIUM, I. S. **https://linux.die.net/man/8/traceroute**. 2018. Disponível em: <https://linux.die.net/man/8/traceroute>.

ELZ, R.; BUSH, R.; BRADNER, S.; PATTON, M. RFC, **Selection and Operation of Secondary DNS Servers**. Fremont, CA, USA: RFC Editor, 1997. 1–11 p. RFC 2182 (Best Current Practice). (Internet Request for Comments, 2182). Disponível em: <https://www.rfc-editor.org/rfc/rfc2182.txt>.

HILTON, S. **Dyn Analysis Summary Of Friday October 21 Attack**. 2016. Dyn blog <https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>.

MCPHERSON, D.; ORAN, D.; THALER, D.; OSTERWEIL, E. RFC, **Architectural Considerations of IP Anycast**. Fremont, CA, USA: RFC Editor, 2014. 1–22 p. RFC 7094 (Informational). (Internet Request for Comments, 7094). Disponível em: <https://www.rfc-editor.org/rfc/rfc7094.txt>.

MIT. **http://web.mit.edu/freebsd/head/contrib/traceroute/traceroute.c**. 2018. Disponível em: <http://web.mit.edu/freebsd/head/contrib/traceroute/traceroute.c>.

MOCKAPETRIS, P. **Domain names - concepts and facilities**. [S.l.], 1987.

MOURA, G. C. M.; SCHMIDT, R. de O.; HEIDEMANN, J.; de Vries, W. B.; MÜLLER, M.; WEI, L.; HESSELMAN, C. Anycast vs. DDoS: Evaluating the November 2015 root DNS event. In: **Proceedings of the ACM Internet Measurement Conference**. [s.n.], 2016. Disponível em: <https://www.isi.edu/%7ejohnh/PAPERS/Moura16b.html>.

MOURA, G. C. M.; SCHMIDT, R. de O.; HEIDEMANN, J.; VRIES, W. B. de; MULLER, M.; WEI, L.; HESSELMAN, C. Anycast vs. ddos: Evaluating the november 2015 root dns event. In: **Proceedings of the 2016 ACM on Internet Measurement Conference - IMC '16**. [s.n.], 2016. ISBN 9781450345262. Disponível em: <http://dl.acm.org/citation.cfm?doid=2987443.2987446>.

PERLROTH, N. **Hackers Used New Weapons to Disrupt Major Websites Across U.S.** 2016. . <https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html>.

POSTEL, J. RFC, **Internet Control Message Protocol**. Fremont, CA, USA: RFC Editor, 1981. 1–21 p. RFC 792 (Internet Standard). (Internet Request for Comments, 792). Updated by RFCs 950, 4884, 6633, 6918. Disponível em: <https://www.rfc-editor.org/rfc/rfc792.txt>.

POSTEL, J. RFC, **Internet Protocol**. Fremont, CA, USA: RFC Editor, 1981. 1–51 p. RFC 791 (Internet Standard). (Internet Request for Comments, 791). Updated by RFCs 1349, 2474, 6864. Disponível em: <https://www.rfc-editor.org/rfc/rfc791.txt>.

RIPE Network Coordination Centre. **RIPE Atlas**. 2018. Disponível em: <https://atlas.ripe.net/>.

Root Server Operators. **Events of 2015-11-30**. 2015. <http://root-servers.org/news/events-of-20151130.txt>.

Root Server Operators. **Events of 2016-06-25**. [S.l.], 2016. Disponível em: <http://www.root-servers.org/news/events-of-20160625.txt>.

SAVARESE. **https://www.savarese.com/software/rocksaw/**. 2018. Disponível em: <https://www.savarese.com/software/rocksaw/>.

SENGUPTA, S. After threats, no signs of attack by hackers. **New York Times**, p. A1, Apr. 1 2012. Disponível em: <http://www.nytimes.com/2012/04/01/technology/no-signs-of-attack-on-internet.html>.

VISSERS, T.; JOOSEN, W.; NIKIFORAKIS, N. **Parking Sensors: Analyzing and Detecting Parked Domains**. 2015. Disponível em: <https://www.securitee.org/files/parking-sensors_ndss2015.pdf>.

Weinberg, M., Wessels, D. **Review and analysis of attack traffic against A-root and J-root on November 30 and December 1, 2015**. 2016. In: DNS OARC 24 – Buenos Aires, Argentina. <https://indico.dns-oarc.net/event/22/session/4/contribution/7>.