MEDIÇÃO, CARACTERIZAÇÃO E REDUÇÃO DOS CUSTOS ASSOCIADOS AO TRÁFEGO DE SPAM

OSVALDO LUÍS HENRIQUES DE MORAIS FONSECA

MEDIÇÃO, CARACTERIZAÇÃO E REDUÇÃO DOS CUSTOS ASSOCIADOS AO TRÁFEGO DE SPAM

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Orientador: Wagner Meira Jr.
Coorientador: Ítalo Cunha

Belo Horizonte
Janeiro de 2016

© 2016, Osvaldo Luís Henriques de Morais Fonseca
Todos os direitos reservados

Ficha catalográfica elaborada pela Biblioteca do ICEx - UFMG

Fonseca, Osvaldo Luís Henriques de Morais I

F676m Medição, caracterização e redução dos custos associados ao tráfego de spam / Osvaldo Luís Henriques de Morais Fonseca — Belo Horizonte, 2016.
xviii, 40 f.: il.; 29 cm.

Dissertação (mestrado) - Universidade Federal de Minas Gerais – Departamento de Ciência da Computação.

Orientador: Wagner Meira Júnior.
Coorientador: Ítalo Fernando Scotá Cunha.

1. Computação – Teses. 2. Spam (Mensagens eletrônicas). 3. Topologia de redes de computadores. 4. Medição de tráfego de redes de computadores. Orientador II. Coorientador. III. Título.

CDU 519.6*74(043)

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FOLHA DE APROVAÇÃO

Medição, caracterização e redução dos custos associados ao tráfego de spam

OSVALDO LUÍS HENRIQUES DE MORAIS FONSECA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

PROF. WAGNER MEIRA JÚNIOR - Orientador
Departamento de Ciência da Computação - UFMG

PROF. ÍTALO FERNANDO SCOTÁ CUNHA - Coorientador
Departamento de Ciência da Computação - UFMG

DRA. CRISTINE HOEPERS
Comitê Gestor da Internet no Brasil

PROF. DORGIVAL OLAVO GUEDES NETO
Departamento de Ciência da Computação - UFMG

DR. KLAUS STEDING-JESSEN
Comitê Gestor da Internet no Brasil

Belo Horizonte, 28 de março de 2016.

Agradecimentos

Agradeço aos meus orientadores, Wagner Meira. Jr e Ítalo Cunha, por todos os ensinamentos, dedicação e paciência em todas as etapas desta dissertação. Foram várias reuniões nos finais de semana, muitos prazos apertados e noites não dormidas para a realização deste trabalho. Agradeço também aos professores Dorgival Guedes e Adriano César, com os quais tive a oportunidade de trabalhar e que sempre se mostraram muito solícitos.

Agradeço aos meus pais, Cornélio e Conceição, que sempre me apoiaram e torceram pelo meu sucesso. Ao meu pai pelo constante incentivo e cuidado para que eu pudesse continuar estudando, principalmente nos momentos mais complicados. Também por ser o melhor amigo que há. À minha mãe por me ensinar e me obrigar a estudar quando era criança, os conhecimentos adquiridos nessa época foram essencias à minha formação.

Agradeço aos meus tios, Carlinhos, Maria Inês, Malu e Cinha por estarem sempre presentes. Agradeço ao pessoal das duas repúblicas, João, Maria Luísa, Gabriel, Samuel e Aline, pelo companheirismo, jantas e conversas; não seria tão agradável estudar até duas horas da manhã sozinho. Agradeço em especial ao meu irmão Gabriel, um amigo inestimável de longa data. Obrigado a todos vocês!

À Alloma pelo companheirismo e compreensão, sempre disposta a ajudar e a me fazer esquecer das preocupações. Também pelo cuidado, preocupação e amor, fazendo o possível para me ver bem. Muito obrigado!

Aos meus amigos do *Speed* por tornarem o ambiente de trabalho o melhor possível. Obrigado a todos pelas conversas e ideias; pela ajuda e paciência; e por tornarem os dias de trabalho mais curtos. Em particular, agradeço aos meus amigos Elverton, Vinícius, Fernandinho, Denise e Samuel, que são amigos que eu vou levar pro doutorado e pós-doutorado da vida.

Agradeço aos colaboradores do CERT.br, Klaus, Cristine e Marcelo, pelo suporte, sugestões e comentários que foram fundamentais para a realização deste trabalho.

Por fim, agradeço a todas as pessoas que, direta ou indiretamente, contribuíram de alguma forma para a realização deste trabalho.

Resumo

Mensagens de *spam* são utilizadas na propagação de *malware*, disseminação de mensagens de *phishing* e na divulgação de produtos ilegais. Essas mensagens geram custos para usuários finais e operadores de rede, mas é difícil mensurar quanto desse custo está associado ao tráfego de *spam* e quem, de fato, paga pelo tráfego. Neste trabalho, propomos uma metodologia para quantificar o custo do tráfego de *spam* para os operadores de rede. Através de máquinas da plataforma RIPE Atlas, realizamos medições de *traceroute* para estimar as rotas percorridas pelas mensagens de *spam* coletadas por cinco *honeypots* de baixa interatividade. Esses coletores simulam máquinas vulneráveis e levam os *spammers* a crerem que estão interagindo com legítimos *relays* e *proxies* abertos. Em seguida, identificamos os Sistemas Autônomos em cada uma das rotas e utilizamos a base de dados de relações comerciais entre ASes para inferir os custos do tráfego de *spam*. Nossos resultados mostram que redes de borda são sistematicamente oneradas pelo tráfego de *spam* e que redes maiores podem receber duas vezes pelo tráfego de uma mesma mensagem. Além disso, mostramos que algumas redes lucram com o tráfego de *spam* e provavelmente não estão motivadas em filtrar essas mensagens de *spam* na origem; outras redes, mesmo pagando pelo *spam*, quando conseguem encaminhar essas mensagens aos seus clientes podem não ter incentivos para filtrá-las. Finalmente, apresentamos um algoritmo simples, porém eficiente para identificar redes que se beneficiariam em cooperar na filtragem de *spam* para reduzir os custos associados ao tráfego de *spam*.

Palavras-chave: Spam, Topologia de rede, Técnicas de medição.

Abstract

Spam messages are often used to propagate malware, to disseminate phishing exploits, and to advertise illegal products. Those messages generate costs for users and network operators, but it is hard to measure how much of their costs are associated with spam traffic, and who actually pays for it. In this work, we provide a method to quantify the transit costs of spam traffic. We issue traceroutes from RIPE Atlas vantage points to estimate the routes traversed by spam messages collected at five honeypots. These collectors simulate vulnerable machines and lead spammers to believe they are interacting with legitimate open relays and proxies. Then we map IP-level traceroute measurements to AS-level paths and use the database of inter-network business relationships to infer the spam traffic costs. Our results show that stub networks are systematically subject to high spam traffic costs and that large ASes can profit twice with the spam traffic of the same message. Furthermore, we show that some networks profit from spam traffic and might not be motivated in filtering spam; other networks, even paying for spam traffic, when they can foward these messages to their customers may not be motivated in filtering them. Finally, we present a simple but effective algorithm to identify the networks that would benefit in cooperating to filter spam traffic at the origin to reduce transit costs.

Keywords: Spam, Network topology, Measurement techniques.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

Mensagens de *spam*, e-mails não solicitados enviados para uma grande quantidade de destinatários, estão frequentemente associadas à propagação de *malware* [Newman et al., 2002], divulgação de produtos ilegais e são também utilizadas para atrair usuários a réplicas falsas de serviços reais (*phishing*) [Orman, 2013]. Mensagens de *spam* representam mais de 66% de todas as mensagens de e-mail e geraram aproximadamente 216 TB de tráfego em 2013 [Symantec, 2014].

A batalha contra os *spammers* é travada em múltiplas frentes. Recentemente, muitos trabalhos têm focado em filtrar o *spam* na origem (e.g., gerência de porta 25), para evitar que as mensagens de *spam* trafeguem pela Internet até as redes de destino, consumindo banda de rede [Las-Casas et al., 2013a; Duan et al., 2012]. Contudo, na prática, o *spam* geralmente é tratado somente nos servidores de e-mail de destino, sendo filtrado pelo conteúdo, evitando que essas mensagens sejam entregues aos usuários.

Um Sistema Autônomo (AS) na Internet é uma entidade registrada junto às autoridades da Internet (RIRs), e.g., ARIN ou LACNIC, como operadora de recursos de rede conectados à Internet, como: roteadores, enlaces, computadores e faixas de endereços IP. Além disso, um AS tem uma política de roteamento única e bem definida. Para obter conectividade global, ASes estabelecem relações para troca de tráfego. Relações comerciais entre ASes podem ser pagas, e.g., quando um AS regional paga para um AS global para ter conectividade, ou livre de cobrança, quando dois ASes concordam em trocar tráfego sem custo para ambas redes. Por causa da natureza dessas relações, enviar e receber mensagens de *spam* pode resultar em custos diretos para ASes que pagam por conectividade.

Existem trabalhos na literatura que mostram que o *spam* gera grandes volumes de tráfego de rede e um alto custo para a Internet, mais de 20 bilhões de dólares todos os anos [Sipior et al., 2004; Rao & Reiley, 2012]. Entretanto, esses trabalhos consideram

apenas o custo agregado e não uma granularidade menor para analisar quais redes são oneradas pelo tráfego de *spam*. Um determinado AS, por exemplo, se alertado que está sendo muito prejudicado pelo tráfego de *spam*, estará mais motivado à adotar mecanismos para filtrar as mensagens de *spam* próximas à origem, evitando os custos associados ao tráfego e abrindo as portas para novos mecanismos de filtragem de *spam* que necessitam do consentimento dos operadores de rede.

Neste trabalho nós avaliamos o custo gerado pelo tráfego de *spam* para cada sistema autônomo. Combinamos o volume das mensagens de *spam*, os caminhos percorridos por elas e as relações entre sistemas autônomos para estimar o custo do tráfego de *spam*. Como os contratos das relações entre ASes são privados, não podemos calcular os custos absolutos do tráfego de *spam*. Desta forma, consideramos o custo do tráfego de *spam* baseado na inferência das relações comerciais entre os ASes e o volume do tráfego de *spam*.

Nossa metodologia de medição nos permite entender quais ASes pagam e quais lucram com o tráfego de *spam*. Utilizando cinco máquinas que se passam por servidores vulneráveis para atrair os spammers (*honeypots*) instaladas em diferentes países, em três continentes, durante 31 dias, observamos o tráfego gerado por 133 milhões de mensagens de *spam* que foram entregues aos *honeypots*. Nós medimos 57.419 rotas percorridas pelas mensagens de *spam* através de medições de *traceroute* realizadas por máquinas do RIPE Atlas, uma plataforma de medição distribuída com mais de 9.000 sensores em diferentes países. Em seguida, mapeamos os endereços IP observados nos *traceroutes* para o AS que originou aquele prefixo IP e depois processamos os caminhos no nível de AS para remover Pontos de Troca de Tráfego (PTTs), pois PTTs não fornecem tráfego por eles mesmo, apenas proveem conectividade entre os ASes [Chen et al., 2009]. Por fim, estimamos o custo do tráfego utilizando a base de dados de relações comerciais da CAIDA [Luckie et al., 2013; Giotsas et al., 2014], que informa se a troca de tráfego para um determinado par de ASes é livre de cobrança (ASes parceiros) ou paga, quando a relação entre os ASes é do tipo cliente-provedor, i.e., o AS regional paga para o AS global para obter conectividade.

Nossos dados mostram que ASes grandes lucram com o tráfego de *spam*, pois trocam tráfego através de ASes clientes ou parceiros. ASes médios, devido à frequente falta de ASes parceiros para encaminhar as mensagens de *spam* em direção aos seus destinos, têm que encaminhar pelo menos algumas mensagens por enlaces com relacionamento do tipo cliente-provedor. Pequenos ASes de borda, pagam integralmente pelo tráfego de *spam*, pois dependem dos seus provedores para obter conectividade global. Curiosamente, ASes que originam grandes quantidades de *spam* têm maiores limitações de conectividade (menor quantidade de ASes parceiros) do que ASes que recebem

pelo *spam*, aumentando o custo do tráfego de *spam* em geral. Isso acontece porque o tráfego tem que subir muito na hierarquia e gera custo para todos os ASes que estão na descida do caminho.

Por fim, propusemos um algoritmo para identificar pares de ASes que poderiam se beneficiar mutuamente e reduzir seus custos filtrando *spam* próximo à origem. O algoritmo utiliza apenas informações públicas disponíveis sobre os ASes e pode ser utilizado pelos ASes ou como um serviço para eles. Nossa metodologia se aplica não somente ao *spam*, mas também a outras fontes de tráfego indesejado, e.g., Ataque de Negação de Serviço Distribuído (DDoS), que utilizam muita banda.

Nossas avaliações mostram que a filtragem pode reduzir significativamente o custo do tráfego de *spam*, mas apenas quando um AS utiliza esse algoritmo para identificar aqueles poucos ASes que também poderiam se beneficiar de tal filtragem e, portanto, estariam dispostos a tomar medidas para bloquear esse tipo de tráfego. Como exemplo, um AS x, que recebe grandes volumes de *spam* através de provedores (i.e., tráfego que gera custo), pode utilizar o algoritmo proposto para identifiar os ASes que pagam para enviar ou encaminhar essas mensagens de *spam*. Assim, o AS x pode pedir a esses ASes para filtrá-las, reduzindo o custo associado ao tráfego para todos os envolvidos. A caracterização que realizamos indica que iniciativas globais contra o *spam* podem desperdiçar esforços em ASes que, em última análise, não estão interessados em filtrar o tráfego de *spam*. Nossas contribuições são aplicáveis e podem ser úteis para serviços de filtragem de *spam* já existentes.

Este trabalho resultou nas seguintes publicações: "Uma Análise do Custo do Tráfego de Spam para Operadores de Rede" no SBRC 2015 [Fonseca et al., 2015] e "Measuring, Characterizing, and Avoiding Spam Traffic Costs" no Internet Computing [Fonseca et al., 2016].

O restante desta dissertação é organizada como segue. O capítulo 2 discute os trabalhos relacionados à medição de rotas, criação de topologias no nível de AS, caracterização do tráfego de *spam* e sobre os custos gerados pelo envio de *spam*. O capítulo 3 detalha a metodologia proposta para estimar o custo do tráfego para operadores de rede. O capítulo 4 apresenta os primeiros resultados através de um estudo de caso para o *honeypot* AT-01 e, em seguida, generaliza esses resultados para os outros *honeypots*. Também é realizada uma caracterização dos ASes responsáveis pela maior parte do tráfego e analisado o efeito de amplificação do tráfego ao chegar nos servidores de e-mail. A proposta de uma algoritmo para identificar ASes com interesse em filtrar o tráfego de *spam* é apresentada no capítulo 5. Por fim, as conclusões e trabalhos futuros são discutidos no capítulo 6.

Capítulo 2

Trabalhos Relacionados

Neste capítulo apresentamos os trabalhos relacionados a esta dissertação. Primeiro evidenciamos os problemas associados à utilização de medições de *traceroute* na criação de topologias no nível de AS (e.g., mapear endereços IP em ASes) e discutimos as abordagens empregadas para inferir as relações entre pares de ASes. Em seguida, apresentamos trabalhos sobre a caracterização de tráfego de *spam* na Internet e estudos que têm como objetivo identificar os *spammers* na origem, evitando o custo gerado por esse tráfego para os operadores de rede. Finalmente, mencionamos os trabalhos sobre o custo associado ao envio de *spam* e os estudos que tratam especificamente do custo relacionado ao tráfego de *spam*.

2.1 Medição de Rotas e Mapeamento em Sistemas Autônomos.

Neste trabalho fazemos uso de técnicas de mapeamento topológico para obter informações sobre as rotas por onde as mensagens de *spam* foram transmitidas. Como as medições de *traceroute*[1] fornecem os caminhos percorridos pelas mensagens de spam na granularidade de IP e precisamos da topologia no nível de AS, é necessário mapear os endereços IP em seus respectivos Sistemas Autônomos. Bases de dados para mapeamento de endereços IP em ASes [Madhyastha et al., 2006] são construídas mapeando prefixos IP para o AS que originou o anúncio BGP (protocolo de políticas de roteamento entre ASes) daquele prefixo. Para maximizar a cobertura do espaço de endereçamento IP, estas bases utilizam anúncios de rotas coletados por diversos rotea-

[1] *Traceroute* é uma ferramenta de medição capaz de identificar sequências de endereços IP (interfaces dos roteadores) que aparecem no caminho entre uma origem e um destino na Internet.

dores BGP conectados à Internet (como os roteadores dos projetos RouteViews [Meyer et al., 2005] e RIPE RIS [RIPE, 2005]) bem como informações de alocação de prefixos dos RIRs (ARIN, LACNIC, RIPE NCC, APNIC e Afrinic).

Uma vez que essas bases de dados não são atualizadas automaticamente e podem conter informações incorretas, o mapeamento de endereços IP em ASes pode inserir erros com frequência [Amini et al., 2002]. Alguns trabalhos propuseram heurísticas para corrigir esses erros e melhorar a precisão do mapeamento de endereços IP em ASes [Chen et al., 2009; Mao et al., 2003]. Em particular, Chen et al. [2009] observaram que endereços IP pertencentes a pontos de troca de tráfego (interconexão física para troca de tráfego entre ASes) podem aparecer entre dois ASes conectados ao PTT e que ASes podem usar endereços IP "emprestados" de outros ASes; ambos levam à criação de parcerias falsas depois que os endereços IP dos *traceroutes* são mapeados para seus respectivos ASes. Além disso, Mao et al. [2003] mostram que heurísticas muito simples podem reduzir em quase 40% o problema de caminhos incompletos. Em nosso trabalho implementamos e utilizamos algumas das heurísticas propostas nesses estudos.

Os primeiros algoritmos para identificação de relações entre ASes foram propostos por Gao [2001], que define três grupos em que essas relações podem ser classificadas: cliente-provedor, parceiros (peer) e ASes *siblings*. Xia & Gao [2004] propõem uma forma de avaliar as relações inferidas e comparam o algoritmo proposto por eles com outros dois algoritmos conhecidos na literatura [Gao, 2001; Subramanian et al., 2002]. Neste trabalho utilizamos a base de dados mais recente à qual temos acesso, disponibilizada pela CAIDA [Luckie et al., 2013]. O algoritmo de inferência da CAIDA utiliza várias regras que capturam técnicas de engenharia de tráfego, práticas de mercado e políticas de roteamento. A base de dados da CAIDA tem precisão de 95% [Luckie et al., 2013] e continua sendo aprimorada [Giotsas et al., 2014].

2.2 Filtragem e Caracterização de Tráfego de Spam na Internet.

Existem vários trabalhos sobre filtragem e caracterização de tráfego na Internet. Estudos iniciais, com a finalidade de filtrar as mensagens de *spam* nos servidores de destino, analisam o conteúdo das mensagens [Sahami et al., 1998; Androutsopoulos et al., 2000; Goodman et al., 2007] e a reputação dos remetentes através de *blacklists* públicas. Contudo, devido a utilização de técnicas sofisticadas para alterar o conteúdo das mensagens, filtros de *spam* que se baseiam no conteúdo podem se tornar menos eficazes ou necessitar de modelos muito complexos. Além disso, estudos recentes mostram o uso

de *bots* pelos *spammers* para confundir os filtros de *spam* colaborativos, se passando por usuários e votando em suas mensagens como sendo legítimas [Ramachandran et al., 2011]. Uma vez que o número de contas de e-mail comprometidas é muito grande, essa atividade consegue confundir os filtros de *spam* e fazê-los classificar, não somente essas, mas também outras mensagens de *spam* como legítimas.

Quanto à utilização de filtros de *spam* baseados em *blacklists*, esses funcionavam bem quando as mensagens de *spam* eram oriundas de endereços IP fixos. Atualmente, como as campanhas de *spam* contam com muitos remetentes, cada um enviando um pequeno número de mensagens para cada domínio, o uso de *blacklists* não é muito eficaz. Assim, surgiram trabalhos que classificam os remetentes através de seus comportamentos de envio, permitindo identificar *spammers* que não seriam detectados por sistemas baseados em *blacklists* e possibilitando essa identificação no início do envio [Ramachandran et al., 2007; Hao et al., 2009]. Mesmo assim, essas abordagens não evitam o desperdício de banda causado pelo tráfego de *spam*, uma vez que essas análises são realizadas depois que as mensagens chegam aos servidores de destino.

Mais próximos do nosso trabalho são estudos sobre a caracterização de propriedades do tráfego de *spam*, que têm como objetivo identificar as diferenças no envio de mensagens de *spam* e mensagens legítimas [Gomes et al., 2004, 2005, 2007; Kim & Choi, 2008; Ramachandran & Feamster, 2006; Venkataraman et al., 2007]. Entre esses, Gomes et al. [2004] fazem uma caracterização do tráfego de *spam* e comparam com o comportamento de mensagens legítimas utilizando as informações contidas no cabeçalho das mensagens. Esse trabalho mostra que existe uma diferença significativa sob vários aspectos do envio entre as duas categorias (e.g., número de destinatários, tamanho das mensagens) e podem ser utilizadas na criação de métodos mais robustos na detecção de *spam*. De forma análoga, Venkataraman et al. [2007] analisam extensivamente os endereços IP que enviam mensagens de *spam* e contrastam com o comportamento daqueles que enviam mensagens legítimas. Além disso, mostram que a maioria dos endereços IP enviam predominantemente um dos dois tipos de mensagens: *spam* ou legítima. Já Ramachandran & Feamster [2006] mostram que alguns elementos (e.g., AS de origem, anúncio de rotas BGP de curta duração) do tráfego de *spam* podem ser utilizados para tentar identificar sua transmissão através da rede. Em particular, o trabalho mostra que o envio de *spam* está concentrado em uma pequena região do espaço de endereçamento IP.

Outros estudos têm como objetivo identificar regiões no espaço de endereçamento IP onde há uma maior concentração de atividades associadas ao envio de *spam* [van Wanrooij & Pras, 2010; Moreira Moura et al., 2011; Fonseca et al., 2014; Konte et al., 2015]. Como esse envio não está igualmente distribuído pela Internet [Ramachandran &

Feamster, 2006], van Wanrooij & Pras [2010] propõem o conceito de *Bad Neighborhoods*, i.e., regiões no espaço de endereçamento IP com um número significativo de máquinas com comportamento malicioso. Os autores propõem uma forma de detectar o *spam* sem analisar todo o conteúdo das mensagens, avaliando basicamente os endereços IP de origem dos e-mails e URLs presentes no corpo das mensagens. Moreira Moura et al. [2011] estende este conceito para se referir a segmentos de rede que enviam grandes volumes de *spam*, independente do número de máquinas envolvidas e da forma de envio dos *spammers*. Mais relacionado a este trabalho, Fonseca et al. [2014] consideram cada Sistema Autônomo como uma vizinhança e identifica aquelas com comportamento malicioso. Desta forma, os autores conseguem identificar quais são as redes onde os esforços no combate ao *spam* devem ser concentrados e onde a instalação de filtros de *spam* seriam mais eficazes. De forma similar, no nosso trabalho propusemos um algoritmo para identificar pares de ASes que se beneficiariam se houvesse cooperação entre eles para filtrar as mensagens de *spam* próximas à origem.

Também relacionados às nossas análises são estudos para combater o envio de *spam* na origem, identificando as máquinas responsáveis por enviar as mensagens de *spam* ou criando alternativas para filtrar essas mensagens na origem [Ramachandran et al., 2007; Hao et al., 2009; Duan et al., 2012; Las-Casas et al., 2013a; Fazzion et al., 2014]. Entre esses, Duan et al., observando as mensagens de saída de uma rede, propõem um sistema para identificar máquinas comprometidas e envolvidas com atividades associadas ao envio de *spam*; o sistema proposto é capaz de identificar a maioria das máquinas comprometidas depois de receber apenas três mensagens. Fazzion et al. [2014] propõem uma técnica, *SpamBands*, que utiliza a coocorrência dos endereços IP nas campanhas de *spam* para identificar grupos de endereços IP que estão trabalhando de forma conjunta para disseminar mensagens de *spam*. Além disso, os autores mostram como a identificação desses grupos ajudaria a melhorar algumas *blacklists* (e.g., XBL Spamhaus). Também, utilizando apenas métricas de rede, Las-Casas et al. [2013a] desenvolveram uma técnica baseada em classificadores supervisionados capaz de identificar *spammers* na fonte; inicialmente, o sistema precisa de uma base de dados que distingue mensagens de *spam* de mensagens legítimas como treino, sendo necessário novas amostras rotuladas a cada mês para manter a eficácia do algoritmo.

Mais importante do ponto de vista deste estudo são trabalhos que usam dados de rotas para identificar ASes maliciosos [Konte & Feamster, 2011; Konte et al., 2015]. Esses trabalhos mostram que a duração dos anúncios BGP, a quantidade de provedores em que um AS já se conectou e a frequência em que ele muda o seu conjunto de provedores são muito diferentes entre ASes maliciosos e ASes legítimos. Ramachandran & Feamster [2006] também avaliam as rotas percorridas pelas mensagens de *spam* para

inferir as localizações dos servidores de e-mail e identificam as regiões do espaço de endereçamento IP onde há uma maior concentração no envio de *spam*. Neste trabalho, além de identificar os ASes com maior atividade (tanto envio quanto recebimento de *spam*), mostramos quais são as redes oneradas por esse tráfego e que podem ter interesse em filtrar as mensagens de *spam* na origem ou no meio da rede.

2.3 Custos de Spam e Tráfego na Internet.

Alguns trabalhos na literatura mostram que o envio de *spam* gera um alto custo para a Internet [Sipior et al., 2004; Rao & Reiley, 2012]. Em particular, Rao & Reiley [2012] estimam que o prejuízo gerado por cada dólar recebido por um *spammer* é de cem dólares; e o prejuízo total para empresas e usuários é estimado em 20 bilhões de dólares. Se o custo gerado pelo tráfego de *spam* para os sistemas autônomos fosse considerado, esses prejuízos seriam ainda maiores. Além disso, esses trabalhos consideram apenas o custo agregado, e não uma granularidade menor que permita inferir quais entidades estão sendo oneradas pelo *spam*. Outros trabalhos tentam entender o mercado que envolve o envio de *spam* e quantificar os recursos usados para monetizá-lo [Anderson et al., 2007; Kanich et al., 2008; Levchenko et al., 2011; McCoy et al., 2012]. Entre esses, Kanich et al. [2008] apresentam uma metodologia para calcular a quantidade de mensagens de *spam* que devem ser enviadas para o *spammer* ter um retorno positivo (e.g., resultar em uma venda). Eles estimam que uma única campanha de *spam* consegue ter um rendimento próximo a 7.000 dólares por dia. Em [Levchenko et al., 2011], os autores visam identificar os gargalos no processo de monetização do *spam*. Estudos como esse têm o potencial de assistir na criação de mecanismos para aumentar os custos para os *spammers*, tornando suas atividades menos rentáveis.

Sobre a questão do custo do tráfego, Anderson et al. [2007] apresentam uma análise do custo da infra-estrutura de envio de *spam*, bem como do custo de conectividade para o *spammer*, mas não há uma análise do impacto desse tráfego no custo operacional dos demais ASes, como buscamos fazer neste trabalho. Também relacionados a esse tema são trabalhos que discutem propriedades do modelo de cobrança comumente utilizado para trânsito na Internet, baseado no 95º percentil do tráfego [Stanojevic et al., 2010; Dimitropoulos et al., 2009]. Esses estudos mostram que cobrança pelo 95º percentil é sensível à parametrização (e.g., duração do intervalo de agregação de tráfego) e que a sensibilidade é maior para redes que trafegam poucos dados (e.g., redes de borda). Mesmo trabalhos mais recentes que consideram novos modelos alternativos para cobrança por trânsito na Internet consideram o volume de tráfego e os enlaces

por onde o dado trafega [Valancius et al., 2011]. Neste trabalho, buscamos quantificar os custos gerados pelo tráfego de *spam* para cada Sistema Autônomo com o intuito de incentivar redes sistematicamente oneradas pelo tráfego a cooperar com a filtragem de *spam* na origem ou próximo a ela. Também mostramos que redes de borda são as mais oneradas pelo tráfego de *spam* e, que, em contrapartida, ASes maiores chegam a receber duas vezes pelo tráfego de uma mesma mensagem (e.g., no recebimento e no encaminhamento da mensagem).

Capítulo 3

Base de Dados e Metodologia

Neste capítulo apresentamos a metodologia criada para estimar o custo gerado pelo tráfego de spam para os operadores de rede. Primeiro descrevemos a coleta das mensagens de spam e relatamos as estatísticas dos dados coletados entre 8 de setembro e 8 de outubro de 2015 (seção 3.1). Em seguida, apresentamos a infraestrutura de medição das rotas percorridas pelas mensagens de spam e o processo de identificação dos sistemas autônomos em cada uma das rotas nas seções 3.2 e 3.3, respectivamente. Finalmente, na seção 3.4, baseado nas relações comerciais entre os ASes, descrevemos o processo utilizado para inferir os custos gerados pelo tráfego de *spam* para os operadores de rede. A figura 3.1 ilustra nossa infraestrutura de medição.

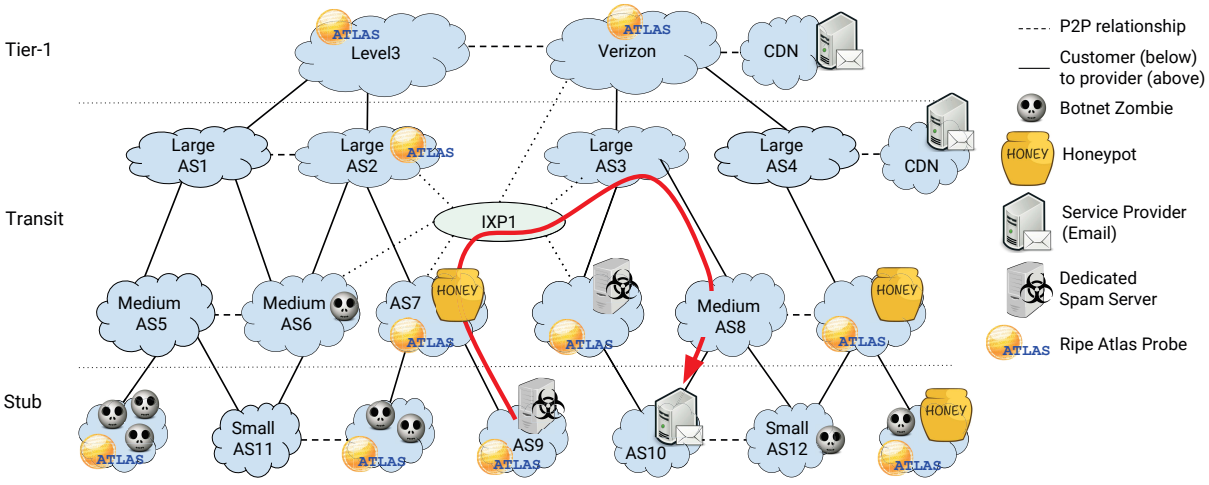

Figura 3.1. Visão geral da infraestrutura de medição. A curva em vermelho mostra a rota percorrida por uma mensagem de *spam* enviada do AS9 para um servidor de e-mail no AS10 passando por nosso *honeypot* localizado no AS7. Clientes (abaixo) pagam para provedores (acima) por tráfego.

3.1 Mensagens de spam e o tráfego global de spam

Coletamos mensagens de *spam* utilizando cinco *honeypots*[1] de baixa interatividade, máquinas que se passam por servidores vulneráveis para atrair os *spammers* [Steding-Jessen et al., 2008]. Os *honeypots* são configurados para simular *proxies* HTTP e SOCKS bem como *relays* SMTP abertos. Esses serviços são frequentemente utilizados para o envio de *spam*. Como os *honeypots* não prestam serviço para nenhuma rede e não são anunciados publicamente, assumimos (e inspeções manuais indicaram) que todas as mensagens de e-mail recebidas vieram de *spammers* que procuravam por *relays* e *proxies* abertos. Nossos *honeypots* nunca encaminham as mensagens de *spam* recebidas, com exceção de mensagens cujo conteúdo indicam que são mensagens de teste usadas pelos *spammers* para verificar se os *relays* e *proxies* abertos estão funcionando [Steding-Jessen et al., 2008]. Dos treze *honeypots* do projeto, trabalhamos com os cinco coletores que estão localizados em redes cobertas pelos sensores RIPE Atlas. Esses *honeypots* estão instalados em cinco países diferentes, um na Áustria, um no Brasil, um nos Estados Unidos, um na Holanda e um no Uruguai.

Toda interação com os *honeypots* é registrada e as mensagens de *spam* armazenadas localmente. Periodicamente, ao longo de cada dia, todo o *spam* armazenado nos *honeypots* é copiado para os servidores centrais do projeto. No período analisado, coletamos 133 milhões de mensagens de *spam* de 56.051 endereços IP localizados em 879 ASes distintos registrados em 115 países. A maioria dos endereços IP (82,02%) enviando *spam* usaram os *honeypots* como *relays* abertos e enviaram poucas mensagens (26,75% do total), comportamento previamente observado como sendo típico de *botnets* [Las-Casas et al., 2013b]. O restante dos endereços IP (17,98%) utilizam os *honeypots* como *proxies* para enviar um número muito grande de mensagens (73,25% do total), comportamento compatível com o de servidores dedicados ao envio de *spam* [Las-Casas et al., 2013b].

A figura 3.1 mostra um servidor dedicado ao envio de *spam* hospedado no AS9 usando nosso *honeypot* no AS7 como um *proxy* para enviar mensagens de e-mail a um destinatário cujo domínio de e-mail está no AS10. A curva vermelha mostra o caminho que uma mensagem de *spam* percorreria caso ela tivesse sido encaminhada pelo nosso *honeypot*.

Apesar dos nossos *honeypots* não encaminharem as mensagens de *spam*, nós consideramos o tráfego que seria gerado se estas mensagens tivessem sido enviadas. O tráfego de saída seria 3.08 vezes maior que o de entrada, uma vez que mensagens de *spam* têm destinatários em múltiplos domínios e uma cópia da mensagem tem que ser

[1] Spampots Project: http://honeytarg.cert.br/spampots/

enviada para cada um desses domínios.

Nossa base de dados representa uma pequena fração do tráfego de *spam* da Internet. Em alguns pontos da análise, quando reportamos o volume do tráfego de *spam*, nós também reportamos entre parênteses uma estimativa do que significariam nossas observações ao extrapolar para o volume de *spam* global. Em particular, multiplicamos o volume de *spam* que observamos por 6.250, a razão entre a estimativa da Symantec do volume de *spam* global [Symantec, 2014] e o volume de *spam* nos nossos dados. Nosso objetivo não é mostrar com precisão o tráfego global de *spam*, mas aproximar em ordem de grandeza o que os ASes provavelmente vão observar da Internet. Para uma melhor cobertura do tráfego de *spam* global, nossa metodologia pode ser aplicada em outras bases de *spam*.

3.2 Medindo as rotas da Internet percorridas pelas mensagens de spam

Realizamos medições de *traceroutes* de máquinas do RIPE Atlas localizadas nos mesmos ASes que nossos *honeypots* em direção a cada domínio de destino observado nas mensagens de *spam*. Não realizamos essas medições diretamente dos *honeypots* para proteger suas identidades. O RIPE Atlas é uma plataforma de medição distribuída com mais de 9.000 sensores e que provê pontos de medição nos ASes que hospedam os cinco *honeypots* analisados.

Para medir as rotas dos *spammers* até os *honeypots*, primeiro nós identificamos os ASes que hospedam cada um dos endereços IP que enviam *spam* para um dos nossos *honeypots*. Em seguida, identificamos as máquinas do RIPE Atlas nesses ASes e realizamos medições de *traceroute* a partir delas. Novamente, para preservar a identidade dos *honeypots*, não emitimos os *traceroutes* diretamente aos *honeypots*; realizamos as medições de *traceroute* para uma máquina do RIPE Atlas (ou para seu primeiro endereço IP acessível) no mesmo AS que o *honeypot*. O RIPE Atlas provê uma boa cobertura (40,05%) dos 879 ASes dos quais recebemos mensagens de *spam*, nos permitindo medir as rotas da maioria (92,26%) das mensagens de *spam* recebidas por nossos *honeypots*. Ao realizar as medições de *traceroute* na mesma direção das rotas percorridas pelas mensagens de *spam*, evitamos incertezas causadas por violação de roteamento baseado em destino e rotas assimétricas [He et al., 2005].

Considerando a infraestrutura retratada na figura 3.1, realizamos medições de *traceroute* de uma máquina do RIPE Atlas no AS9 para uma outra máquina do RIPE Atlas no AS7, depois de um nó do RIPE Atlas no AS7 até o servidor de e-mail do

domínio que aparece no destinatário da mensagem. A curva vermelha mostra as rotas medidas.

Uma limitação é que o RIPE Atlas impõe limites rígidos para as taxas de medições, que nos impedem de medir todas as rotas dos *spammers* aos *honeypots* e dos *honeypots* a todos os destinos. Nós trabalhamos com uma cota de 500 medições de *traceroute* por *honeypot* por dia. Para maximizar a utilidade da nossa cota de medições, nós realizamos medições de *traceroute* para cada *honeypot* partindo das máquinas do RIPE Atlas localizadas nos 50 ASes que mais enviaram *spam* para aquele *honeypot* e que são cobertos pelo RIPE Atlas. Para cada *honeypot*, também selecionamos os 450 destinos que mais receberiam *spam* daquele *honeypot*. Assim, computamos novamente o conjunto de ASes e domínios de destino que mais enviaram e receberiam *spam* diariamente baseado nas mensagens de *spam* coletadas no dia anterior.

Como o número de mensagens enviadas e recebidas está concentrado em poucos ASes e poucos domínios de destino, respectivamente, nossa cota diária de medições nos permite uma cobertura de mensagens expressiva. Durante o período analisado, conseguimos cobrir em média 92,25% das mensagens que saem dos *spammers* em direção aos *honeypots* com variações muito discretas, uma vez que o conjunto de *spammers* é estável durante o período de um mês. Também conseguimos cobrir 69,53% das mensagens que seriam encaminhadas pelos *honeypots* até os destinos, com desvio padrão de 25,69% para os diferentes dias, pois as campanhas de *spam* e o conjunto de domínios de destino mudam ao longo do mês.

3.3 Mapeamento dos traceroutes para as rotas no nível de AS

Mapeamos as medições de *traceroute* em nível de IP para caminhos no nível de AS usando a base de dados do iPlane [Madhyastha et al., 2006] de mapeamento de IP em AS, que mapeia um prefixo IP para o conjunto de ASes que origina aquele prefixo. Se um roteador não está respondendo ou se um endereço IP não está mapeado para nenhum AS, mas está entre roteadores com endereços IP mapeados para um mesmo AS, e.g., $[\cdots, \mathrm{AS}_1, x, \mathrm{AS}_1, \cdots]$, mapeamos o endereço IP para AS_1.

Se um roteador não está respondendo ou um endereço IP não está mapeado para nenhum AS, mas está entre roteadores com endereços IP mapeados para ASes diferentes, e.g., $[\cdots, \mathrm{AS}_1, x, \mathrm{AS}_2, \cdots]$, assumimos que o tráfego flui do AS_1 para o AS_2. Isto acontece em 4,59% dos caminhos. Essa suposição pode impactar na completude dos resultados (quando x não está no AS_1 e nem no AS_2), mas nunca impacta na corretude

dos nossos resultados, uma vez que os dados fluem, mesmo que indiretamente, entre AS_1 e AS_2. Se um *traceroute* não chega ao destino, consideramos a rota até o último *hop* medido.

No exemplo mostrado na figura 3.1, convertemos a medição de *traceroute* emitida de uma máquina do RIPE Atlas no AS7 para o seguinte caminho no nível de AS $[AS_7, IXP_1, AS_3, AS_8, AS_{10}]$. Se todos os roteadores no AS_8 não respondem ou tem endereços IP que não puderam ser mapeados, nós obteríamos $[\cdots, AS_3, AS_{10}]$.

Nós usamos a tabela BGP obtida de um dos ASes que hospedam um dos nossos *honeypots* para avaliar a qualidade do nosso método de mapeamento. Comparamos os caminhos no nível de AS obtidos com o processo de mapeamento descrito anteriormente para as rotas de um de nossos *honeypots* com os (verdadeiros) caminhos no nível de AS retirados da tabela de roteamento BGP utilizada pelo AS em que o *honeypot* está hospedado. Observamos que 89,16% dos caminhos no nível de AS obtidos pelo mapeamento de IP em AS foram idênticos aos caminhos da tabela BGP e que 99,39% deles tinham apenas um AS diferente. Não fizemos essa mesma análise para os outros *honeypots* pois não temos acesso às tabelas de roteamento BGP dos ASes hospedando os outros *honeypots*.

3.4 Calculando os custos do tráfego de spam

Identificamos quais ASes pagam e quais lucram com o tráfego de *spam* utilizando a base de dados de relações entre ASes da CAIDA [Luckie et al., 2013; Giotsas et al., 2014]. A base de dados da CAIDA classifica as relações entre ASes como cliente-provedor ou parceiros. Assumimos que clientes pagam a provedores para alcançar conectividade global, e parceiros trocam tráfego livre de cobranças. Essas suposições são comuns na literatura [Luckie et al., 2013].

A base de dados da CAIDA não lista relações entre ASes de trânsito e pontos de troca de tráfego. Entre outros motivos, PTTs não fornecem tráfego por eles mesmos, apenas proveem conectividade entre ASes. Neste trabalho, estamos interessados nas relações entre os ASes que trocam tráfego nos PTTs. Construímos uma lista com prefixos IP e números de ASes utilizados na Internet como pontos de troca de tráfego combinando dados do PeeringDB e trabalhos anteriores [Augustin et al., 2009; Luckie et al., 2013]. Nós removemos esses prefixos IP dos *traceroutes* e números de ASes dos caminhos no nível de AS. Também identificamos dez parcerias com provedores de conteúdo (Google, Amazon e Microsoft) que não estavam presentes na base de dados de relações da CAIDA. Essas parcerias apareciam em 2,30% dos caminhos no nível de AS

(8,14% das mensagens). Assim, rotulamos manualmente estas relações como parcerias livres de cobrança por troca de tráfego. Com essas modificações, a base de dados da CAIDA contém 97,85% de todas as relações entre ASes que apareceram nas nossas rotas no nível de AS e podem resolver todas as relações em 93,73% dos caminhos no nível de AS, cobrindo 99,33% das mensangens observadas.

Na topologia exemplo da figura 3.1, posicionamos provedores acima de clientes e mostramos relações do tipo cliente-provedor com linhas contínuas. Mostramos parcerias sem cobrança por troca de tráfego com linhas tracejadas na horizontal. Nós removemos IXP_1 do caminho no nível de AS antes de calcular o custo do tráfego. Desta forma, os pagamentos iriam fluir do AS_9 para o AS_7 e do AS_7 para o AS_3, e do AS_{10} para o AS_8 e do AS_8 para o AS_3. Mostramos as redes provedoras de conteúdo como parceiros da Verizon e do AS_4.

Capítulo 4

Custo do Tráfego de Spam

Neste capítulo apresentamos nossas descobertas sobre o custo do tráfego de *spam* e mostramos os resultados obtidos através da metodologia apresentada no capítulo 3. Nós estimamos o custo do tráfego de *spam* para cada AS. Como os contratos das relações comerciais entre os ASes são privados, não conseguimos determinar quanto cada *byte* custa para cada AS. Assim, fomos conservadores e não fizemos nenhuma suposição quanto ao custo do tráfego, mas estimamos o custo do tráfego de *spam* como o volume de *spam* trafegado entre provedores e clientes (a troca de tráfego entre parceiros é livre de cobrança).

Para não comprometer a identidade dos *honeypots* omitimos suas localizações exatas e anonimizamos as redes hospedeiras. Primeiro apresentamos um estudo de caso de um *honeypot* na Áustria, AT-01 (seção 4.1). Este estudo de caso, além de ilustrar como a análise de resultados foi feita, revela importantes conclusões práticas de como filtros bem colocados na rede podem bloquear grande parte do *spam* mais próximo à origem. Em seguida, generalizamos os resultados encontrados para os outros *honeypots*, mostrando que os resultados são aplicáveis para o tráfego de *spam* em geral. Também mostramos que, das redes que hospedam os nossos *honeypots*, as maiores têm custos menores que as demais, justamente por terem mais parceiros e conseguirem encaminhar, livre de cobrança, algumas mensagens de *spam*. Finalmente, levando em consideração o tamanho dos ASes, estudamos o *tráfego líquido de spam*, o custo final para cada uma das redes, isto é, o volume de tráfego trocado com os clientes subtraído do volume de tráfego trocado com os provedores.

4.1 Estudo de caso do honeypot AT-01

O mapa da figura 4.1 mostra os ASes que aparecem nas rotas percorridas pelas mensagens de *spam* enviadas pelos *spammers* ao *honeypot* AT-01 e que trafegam uma porcentagem significativa do volume de *spam* gerado. A direção das arestas mostra o sentido do *traceroute* e o tipo de linha a relação comercial. As variáveis sobre as arestas mostram a porcentagem do volume de *spam* indo em direção ao *honeypot* que passa por aquela aresta.

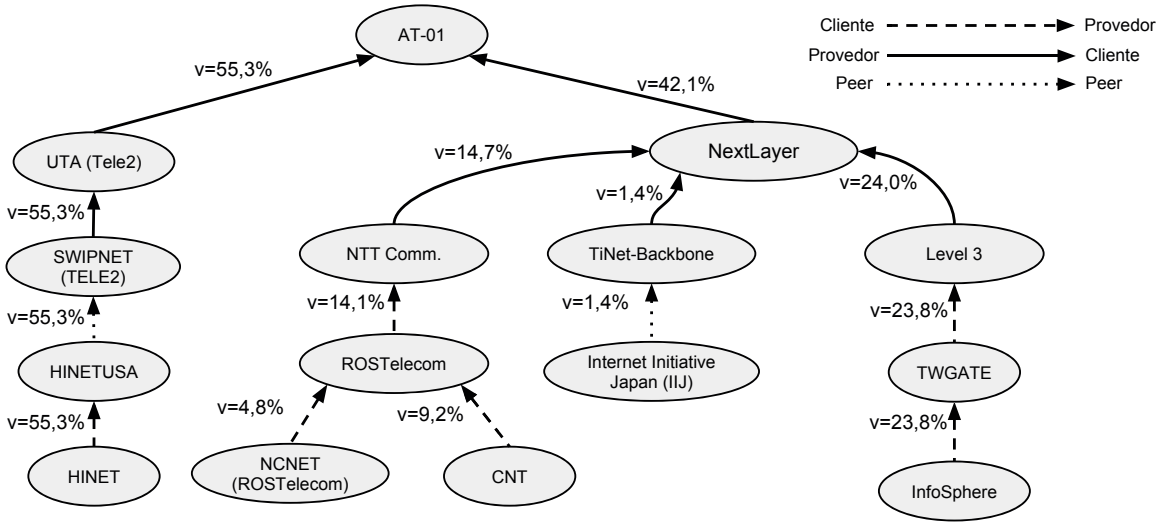

Figura 4.1. Mapa dos ASes mais utilizados entre as máquinas que enviam *spam* e o *honeypot*

A figura 4.1 contém alguns pontos interessantes. O primeiro é a aresta entre o AS do *honeypot* AT-01 e um de seus provedores, a NextLayer (AS1764), onde 42,1% do volume trafega. Apesar da NextLayer, que é uma rede regional, cobrar por todo esse volume, ela tem que pagar aos seus provedores para receber essas mensagens de *spam*. O segundo ponto de interesse são os ASes NTT Comm. (AS2914) e Level3 (AS3356), que lucram duas vezes pelo envio de uma mensagem. A Level3, por exemplo, lucra ao receber do TWGATE (AS9505) 23,8% do tráfego e lucra novamente para encaminhar esse mesmo volume para a NextLayer. Esses ASes, do ponto de vista do custo associado ao tráfego, não têm interesse em filtrar as mensagens de *spam* próximas à origem.

Finalmente, o terceiro ponto de interesse é a HINET (AS3462), que é responsável pelo envio de 55,3% de todo o tráfego de *spam* que chega ao *honeypot* AT-01. Como todo o tráfego que sai da HINET (AS3462), localizada em Taiwan, passa pela HINETUSA (AS9680), apesar da aresta indicar uma relação cliente-provedor, acreditamos que nenhum custo é gerado pois a HINET é filial da HINETUSA. Como a aresta entre

a HINETUSA (AS9680) e a SWIPNET (AS1257) indica uma relação sem cobrança, todo este volume de *spam* que sai da HINET em direção ao AS do *honeypot* AT-01 não tem nenhum custo para a HINET. A InfoSphere, por outro lado, paga integralmente à TWGATE pelo tráfego gerado pelas mensagens de *spam* enviadas de sua rede.

Alguns ASes (e.g., HINET) não tem incentivo econômico em filtar o tráfego de *spam*, pois conseguem enviar mensagens de *spam* sem gerar custo para suas redes. Apesar disso, como podemos observar no mapa da figura 4.1, a instalação de filtros de *spam* em um número pequeno de redes, considerando apenas aquelas sistematicamente oneradas, reduziria bastante o custo do tráfego de *spam* e beneficiaria não somente essas redes. Caso fossem instalados filtros em apenas dois ASes, CNT (AS8615) e InfoSphere (AS2514), 33,0% do tráfego que chega ao AS do *honeypot* AT-01 seria bloqueado na origem. Assim, além de evitar o custo gerado pelo tráfego de *spam* para as redes nas quais os filtros foram instalados, o AS do *honeypot* AT-01 pagaria por 33,0% menos do volume de *spam* que chega até ele.

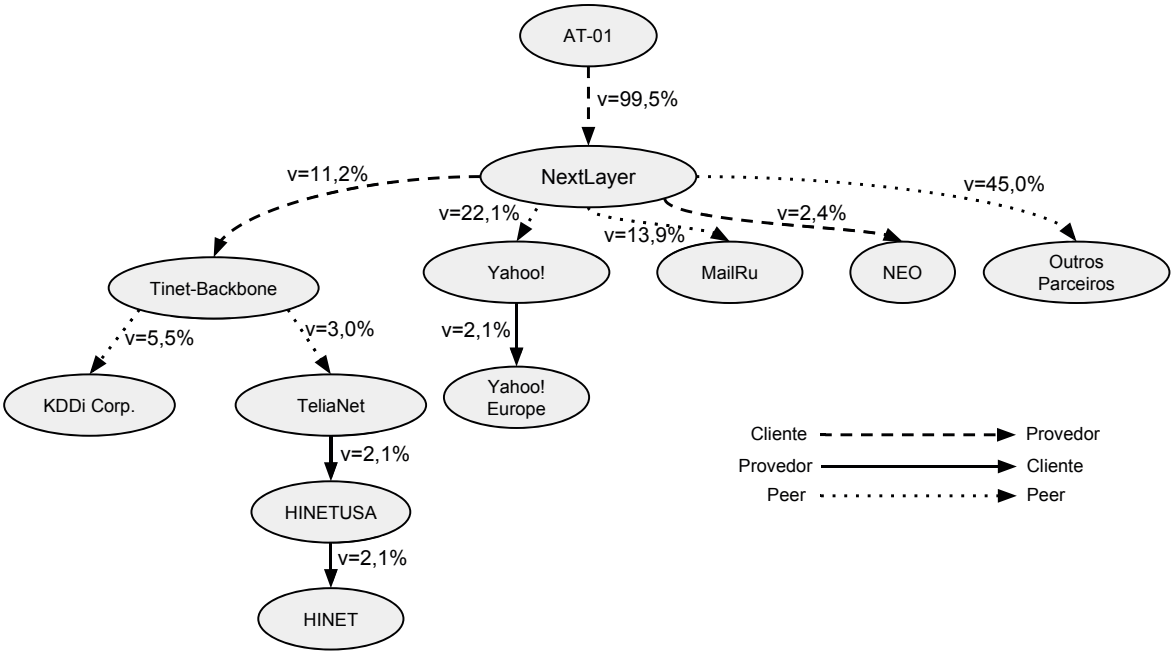

Figura 4.2. Mapa dos ASes mais utilizados entre o *honeypot* e os domínios de destino

O mapa da figura 4.2 é similar ao mapa da figura 4.1, porém mostra os ASes que carregariam o maior volume de tráfego de *spam* enviado pelo *honeypot* até os destinatários, caso as mensagens tivessem sido encaminhadas. Conforme será analisado (seção 4.5), o volume de saída do *honeypot* é maior que o de entrada, pois mensagens com vários destinos precisam ser replicadas pelo menos uma vez para cada domínio

com destinatários. Em outras palavras, o volume de tráfego que circula entre os ASes mostrados na figura 4.2 é maior que o tráfego que circula entre os ASes mostrados na figura 4.1.

De acordo com o mapa da figura 4.2, temos que o *honeypot* AT-01 transmitiria 99,5% do volume de *spam* pela NextLayer. Além disso, como mais de 81,0% do tráfego que chega na NextLayer seria encaminhado a ASes parceiros, essa rede iria receber por 99,5% do volume que sairia do AS do *honeypot* AT-01 e pagaria para seus provedores por menos de 20% desse volume. Esse fato é influenciado pelo tamanho do *customer cone* (i.e., o número de ASes que podem ser alcançados sem a necessidade de um provedor) da NextLayer (352 ASes), que permite a essa rede encaminhar tráfego para diversos outros ASes sem custo.

4.1.1 Análise de custo do honeypot AT-01

As rotas dos mapas mostrados nas figuras 4.1 e 4.2 incitam um questionamento pertinente sobre quem paga e quem recebe pelo tráfego de *spam* gerado. As tabelas 4.1 e 4.2 mostram os principais ASes que são onerados e os principais ASes que lucram com esse volume de *spam*. Para realizar essa análise consideramos as relações comerciais entre os ASes dessas rotas. Para relações cliente-provedor contabilizamos custo para o cliente e lucro para o provedor, proporcionais à quantidade de tráfego. Note que um provedor pode receber por um volume de tráfego maior do que o volume de tráfego total que chega ao *honeypot* caso ele receba o tráfego de um cliente e repasse a outro cliente, como já mencionado anteriormente. Para relações de parceria e relações não inferidas, nenhum tipo de contagem é realizada. Nesse caso, o *honeypot* pode pagar por menos tráfego do que o recebido se parte do tráfego chegar por um AS parceiro. Os resultados de nossa análise consideram o volume de tráfego porque desconhecemos a relação contratual entre os sistemas autônomos (i.e., precificação da banda e condições de uso); não podemos estimar o valor monetário que um AS está pagando ao outro. Notamos que apesar dessa ser uma limitação do nosso trabalho, essa informação é sensível e provavelmente protegida por acordo de sigilo (NDAs) entre as partes.

A tabela 4.1 mostra os cinco ASes que mais pagaram e os que mais lucraram com o tráfego que sai dos *spammers* em direção ao *honeypot* AT-01. Como esperado, o AS que mais pagou, em tráfego, foi o AS do *honeypot* AT-01. Ao aprofundar nas análises dos ASes que mais pagam, percebemos que dois deles, Tele2 (AS8437) e HINET (AS3462), não estão de fato pagando pelo tráfego de *spam*, porque apesar da relação com seus provedores terem sido inferidas como cliente-provedor, acreditamos que os supostos provedores pertencem à mesma organização que seus clientes. De

Tabela 4.1. ASes que mais pagam/recebem no AT-01 nas rotas entre os *spammers* e o *honeypot*

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* AT-01	131,6	TELE2, SE (1257)	74,5
Tele2, AT (8437)	74,5	HINETUSA, TW (9680)	86,8
HINET, TW (3462)	74,5	Tele2, AT (8437)	74,5
NextLayer, AT (1764)	54,4	Level3, US (3356)	64,5
TWGATE, TW (9505)	32,1	NextLayer, AT (1764)	56,8

forma análoga, seus provedores, TELE2 (AS1257) e HINETUSA (AS9680), não estão recebendo pelo tráfego de *spam*. Além disso, como todo o tráfego que a NextLayer e a TWGATE pagam a seus provedores é cobrado de seus clientes (AS do *honeypot* AT-01 e InfoSphere, repectivamente), dos cinco ASes na tabela 4.1, apenas o AS do *honeypot* AT-01 é de fato onerado pelo tráfego de *spam*. Levando em consideração esses aspectos, a Level3 e a TELE2 são os ASes que mais lucram com o tráfego de *spam* nas rotas entre os *spammers* e o *honeypot* AT-01.

A tabela 4.2 mostra os ASes que mais perderam e os que mais ganharam com o tráfego de *spam* que sairia do *honeypot* AT-01 em direção aos servidores de e-mail. A NextLayer recebe por todo o tráfego que sai do AS do *honeypot* AT-01 e consegue encaminhar boa parte das mensagens de *spam* utilizando parcerias. Com isso, apesar de pagar por 52,0 GB de tráfego, recebe por mais de 300,0 GB. Ao comparar as tabelas 4.1 e 4.2, percebemos o efeito de amplificação mencionado anteriormente. O AS do *honeypot* AT-01 paga por 131,60 GB para receber as mensagens de *spam* e 301,60 GB para encaminhá-las em direção aos servidores de destino. Assim, o custo para encaminhar essas mensagens é 229,1% maior que o custo para recebê-las, aumentando ainda mais os custos de comunicação.

Tabela 4.2. ASes que mais pagam/recebem no AT-01 nas rotas entre o *honeypot* e os servidores de destino

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* AT-01	301,6	NextLayer, AT (1764)	301,6
NextLayer, AT (1764)	52,0	Tinet Spa, DE (3257)	39,2
Yahoo! Europe, CH (42173)	16,8	RETN Limited, UA (9002)	27,2
Rambler, RU (24638)	15,4	Yahoo!, US (10310)	16,8
ROSTelecom, RU (12389)	14,6	ROSTelecom, RU (12389)	12,5

4.2 Análise geral dos honeypots

Nesta seção estendemos o estudo de caso feito na seção anterior para os outros quatro *honeypots* (BR-01, NL-01, US-03, UY-01). A tabela 4.3 mostra os ASes que mais foram onerados e os que mais receberam, por *honeypot*, nas rotas trafegadas pelas mensagens enviadas por *spammers* aos *honeypots*. Como podemos notar, com exceção do US-03, os ASes dos *honeypots* são os mais onerados, indicando que, geralmente, ASes que recebem *spam* são os mais prejudicados, porque não podem escolher por qual rota irão receber essas mensagens, sendo na maioria das vezes por provedores que irão se beneficiar desse tráfego.

Tabela 4.3. ASes que mais pagam e recebem, por *honeypot*, pelo tráfego do *spammer* ao *honeypot*

ID	MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AT-01	AS *Honeypot* AT-01	131,6	TELE2, SE (1257)	74,5
	Tele2, AT (8437)	74,5	HINETUSA, TW (9680)	86,8
	HINET, TW (3462)	74,5	Tele2, AT (8437)	74,5
	NextLayer, AT (1764)	54,4	Level3, US (3356)	64,5
	TWGATE, TW (9505)	32,1	NextLayer, AT (1764)	56,8
BR-01	AS *Honeypot* BR-01	83,0	Embratel,BR (4230)	83,0
	Embratel, BR (4230)	81,8	PCCW Global, US (3491)	56,4
	Uninet S.A., MX (28513)	56,4	Uninet S.A., MX (28513)	56,4
	HINET, TW (3462)	56,1	HINETUSA, TW (9680)	56,1
	ROSTelecom, RU (12389)	5,7	Level3, US (3356)	14,5
NL-01	AS *Honeypot* NL-01	134,2	NORDUNET, NO (2603)	86,8
	HINET, TW (3462)	86,8	HINETUSA, TW (9680)	86,8
	InfoSphere, JP (2514)	40,9	KPN Eurorings, NL (286)	40,9
	OCN NTT, JP (4713)	3,9	TWGATE, TW (9505)	40,9
	EGIHosting, US (18779)	1,0	Tinet Spa, DE (3257)	6,5
US-03	HINETUSA, TW (9680)	48,1	Level3, US (3356)	53,3
	HINET, TW (3462)	48,1	HINETUSA, TW (9680)	48,1
	AS *Honeypot* US-03	40,6	Time Warner, US (7843)	40,7
	QuadraNet, US (8100)	17,1	TeliaNet, SE (1299)	18,3
	ROSTelecom, RU (12389)	15,4	PCCW Global, US (3491)	17,1
UY-01	AS *Honeypot* UY-01	64,6	Wholesale Services, ES (12956)	64,6
	HINET, TW (3462)	28,0	SprintLink, US (1239)	28,8
	TWGATE, TW (9505)	20,7	Level3, US (3356)	22,5
	InfoSphere, JP (2514)	20,7	TWGATE-AP, TW (9505)	20,7
	ROSTelecom, RU (12389)	5,3	TeliaNet, SE (1299)	6,1

Como mencionamos, o AS do *honeypot* US-03 tem comportamento diferente dos demais e paga por uma porcentagem menor do volume de tráfego que chega até ele. Ao analisar esse AS, observamos que o tamanho do seu *customer cone* (82 ASes) é mais de três vezes superior a qualquer um dos ASes que hospedam os nossos outros

honeypots. Isso significa que esse AS consegue alcançar um número maior de redes passando apenas por ASes clientes ou parceiros, ou seja, conseguem trocar tráfego com um maior número de ASes sem gerar custos. Isso explica o fato de 56,8% do tráfego chegar até o *honeypot* US-03 sem nenhum custo para a rede que o hospeda.

Um outro fato relevante é a presença da HINET (AS3462) para todos os *honeypots* na tabela 4.3, pois como já foi explicado, a maior parte do tráfego vai para a HINETUSA (AS9680) e ambas redes pertencem a uma mesma organização. Dessa forma, para alguns *honeypots* (AT-01, BR-01 e NL-01), a HINETUSA (AS9680) consegue encaminhar *spam* utilizando parcerias, fazendo com que essas mensagens saiam da HINET sem nenhum custo. Assim, nossos resultados conseguem explicar porque a HINET já foi reportada como sendo um refúgio para os *spammers* e permanece assim: a HINET pode cobrar dos spammers e encaminhar a maior parte do tráfego de spam sem custo. No *honeypot* US-03, a HINETUSA tem que pagar aos seus provedores para encaminhar as mensagens. De forma similar, no *honeypot* UY-01, a HINET encaminha o tráfego para outro provedor, SprintLink (AS1239). Nesses dois últimos, a HINET tem que pagar pelo tráfego de *spam*, mas é uma porcentagem pequena comparada ao volume de mensagens de *spam* que saem da HINET (AS3462) sem custo e chegam aos outros *honeypots*.

A tabela 4.4 mostra o mesmo tipo de informação que a tabela 4.3 para as rotas trafegadas pelas mensagens que seriam enviadas dos *honeypots* aos servidores de destino. O tráfego pago pelos ASes dos *honeypots* nas duas tabelas seguem o mesmo padrão, mas em geral o volume de tráfego na tabela 4.4 é consideravelmente maior devido à amplificação do tráfego ao atingir servidores SMTP. Esse resultado reforça a ideia de como o uso de filtros de *spam* que impeçam as mensagens de atingir os servidores SMTP podem ajudar a reduzir o tráfego na rede. O impacto seria maior do que o gerado pela utilização de filtros em servidores de destino que não impedem as mensagens de percorrer toda rede consumindo recursos.

O AS do *honeypot* NL-01, ao contrário dos outros, paga por um volume menor de *spam* nas rotas entre o *honeypot* e os servidores de destino, apenas 64,8 GB, como pode ser observado na tabela 4.4. Enquanto isso, nas rotas das mensagens enviadas pelos *spammers* até o *honeypot* (tabela 4.3) o tráfego é igual a 134,2 GB, mais de duas vezes superior. Essa redução drástica no volume de *spam* pago pelo AS do *honeypot* acontece porque mais de 40% do tráfego que sairia do *honeypot* em direção aos servidores de destino é encaminhado a ASes parceiros, como mostra a figura 4.3. Isso provavelmente está relacionado com o tamanho do *customer cone* do AS do *honeypot* NL-01, o segundo maior entre os ASes que hospedam os *honeypots*, cujo valor é igual a 26. Isso implica, indiretamente, em um maior número de clientes e parceiros. É importante mencionar

Tabela 4.4. ASes que mais pagam e recebem, por *honeypot*, por tráfego do *honeypot* aos servidores de destino

ID	MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
	AS *Honeypot* AT-01	301,6	NextLayer, AT (1764)	301,6
	NextLayer, AT (1764)	52,0	Tinet Spa, DE (3257)	39,2
AT-01	Yahoo! Europe, CH (42173)	16,8	RETN Limited, UA (9002)	27,2
	Rambler LLC, RU (24638)	15,4	Yahoo!, US (10310)	16,8
	ROSTelecom, RU (12389)	14,6	ROSTelecom, RU (12389)	12,5
	AS *Honeypot* BR-01	323,1	Embratel, BR (4230)	323,1
	Embratel, BR (4230)	105,3	RETN Limited, UA (9002)	118,2
BR-01	MailRu, RU (47764)	57,5	Tinet Spa, DE (3257)	78,3
	Yandex LLC, RU (13238)	29,8	TeliaNet, SE (1299)	41,3
	ROSTelecom, RU (12389)	21,1	Level3, US (3356)	28,6
	AS *Honeypot* NL-01	64,8	NORDUNET, NO (2603)	64,4
	Yahoo! Europe, CH (42173)	17,1	Yahoo!, US (10310)	17,1
NL-01	HiNet, TW (3462)	7,7	HinetUSA, TW (9680)	7,7
	GigaInfra, JP (17676)	3,1	Hurricane Electric, US (6939)	3,1
	Yahoo Japan, JP (23816)	1,6	GigaInfra, JP (17676)	3,1
	RETN Limited, UA (9002)	100,1	Level3, US (3356)	430,0
	MailRu, RU (47764)	92,4	RETN Limited, UA (9002)	99,2
US-03	AS *Honeypot* US-03	79,3	Time Warner, US (7843)	51,1
	Yahoo!, US (10310)	56,8	RASCOM, RU (20764)	50,6
	RASCOM, RU (20764)	50,7	Cable&Wireless Worldwide, UK (1273)	32,9
	AS *Honeypot* UY-01	291,0	Level3, US (3356)	289,1
	RETN Limited, UA (9002)	69,2	Cogent, US (174)	142,2
UY-01	MailRu, RU (47764)	56,4	NTT America, US (2914)	123,7
	RASCOM, RU (20764)	36,2	RETN Limited, UA (9002)	68,5
	Yandex LLC, RU (13238)	34,8	RASCOM, RU (20764)	35,8

que isso acontece apenas para o tráfego saindo do *honeypot*, que é o momento em que o AS do *honeypot* pode optar pelos caminhos que geram o menor custo para ele, ou seja, encaminhar o máximo de mensagens por ASes clientes ou parceiros.

Por último, apontamos alguns ASes que apresentam um comportamento interessante, pois, apesar de estarem entre os cinco ASes que mais pagam pelo tráfego de *spam*, o volume pelo qual eles recebem é sempre maior. A NextLayer é um ótimo estudo de caso neste cenário, visto que o volume de tráfego pelo qual ela recebe é 580,0% maior que o volume pago. Essa rede aparece como provedor direto do AS do *honeypot* AT-01 e aparece na tabela 4.4 pagando por 52,0 GB de tráfego, mas recebe por 301,6 GB. A NextLayer consegue reduzir os custos e obter lucro trafegando as mensagens de *spam* através de algumas parcerias de troca de tráfego com a Yahoo!, MailRu e outras redes (figura 4.2). A Embratel, no *honeypot* BR-01, apresenta um comportamento semelhante, mas em uma proporção menor, recebendo três vezes mais do que paga, como

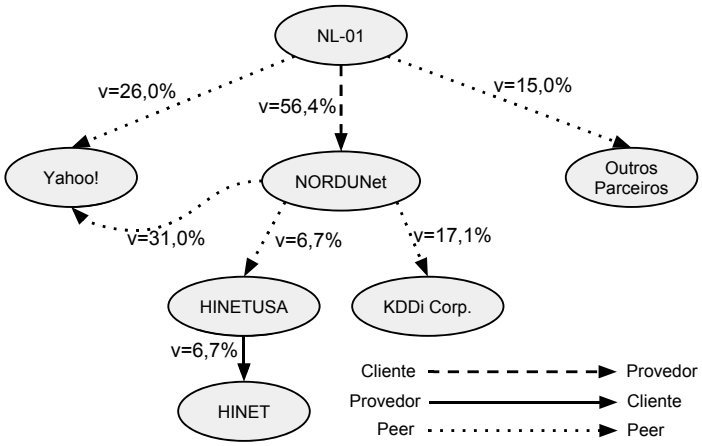

Figura 4.3. Mapa dos ASes mais utilizados entre o *honeypot* NL-01 e os domínios de destino

pode ser observado na tabela 4.4.

4.3 Análise do tráfego líquido de spam

Os ASes lucram pela troca de tráfego de *spam* com seus clientes e pagam com a troca de tráfego de *spam* com os seus provedores. Nós estudamos o *tráfego líquido de spam* para cada um dos ASes, o volume de tráfego trocado com os clientes subtraído do volume de tráfego trocado com os provedores. Um AS com *tráfego líquido de spam* positivo implica que o Sistema Autônomo lucra com o tráfego de *spam*. Por outro lado, um AS com *tráfego líquido de spam* negativo paga pelo tráfego.

A figura 4.4 mostra a mediana e os quartis (blocos), os percentis 5% e 95% (linhas tracejadas) e também alguns ASes com valores extremos de *tráfego líquido de spam* (*outliers*) que aparecem na nossa base. Note a escala logarítimica no eixo y. Nós classificamos os ASes pelo tamanho de seus *customer cones*, o número de outros ASes que podem ser alcançados sem a necessidade de um provedor (i.e., através de enlaces com parceiros ou de clientes) [Luckie et al., 2013]. Notamos que a maioria dos ASes pagam/recebem por um pequeno volume de tráfego de *spam*. Para focar em ASes significativamente impactados pelo tráfego de *spam*, a figura 4.4 não inclui ASes com taxa média de *tráfego líquido de spam* inferior a ±16 Kbps (±100 Mbps depois de multiplicar por 6250 para dimensionar para o volume de *spam* global [Symantec, 2014]).

ASes grandes, com mais de 100 ASes em seus *customer cones*, raramente pagam e frequentemente lucram com o tráfego de *spam*. Isso porque esses ASes lucram com a

troca de tráfego com seus clientes e encaminham o tráfego de *spam* através de parcerias livre de cobrança. A Level3 (AS3356) trafega 28,17% das mensagens de *spam* da nossa base de dados e lucra com uma taxa de *tráfego líquido de spam* de 2.77 Mbps (17.36 Gbps). É importante enfatizar que ASes maiores podem lucrar duas vezes com o tráfego de *spam*, sempre que eles recebem mensagens de seus clientes e encaminham a outros clientes. Esses, do ponto de vista do tráfego de *spam*, não têm nenhum incentivo para cooperar na filtragem do envio de *spam*.

ASes médios, incluindo entre 10 e 100 ASes em seus *customer cones*, raramente lucram com o tráfego de *spam* e comumente pagam pelo tráfego de *spam*. Os ASes médios pagam pelo tráfego de *spam* em duas situações:

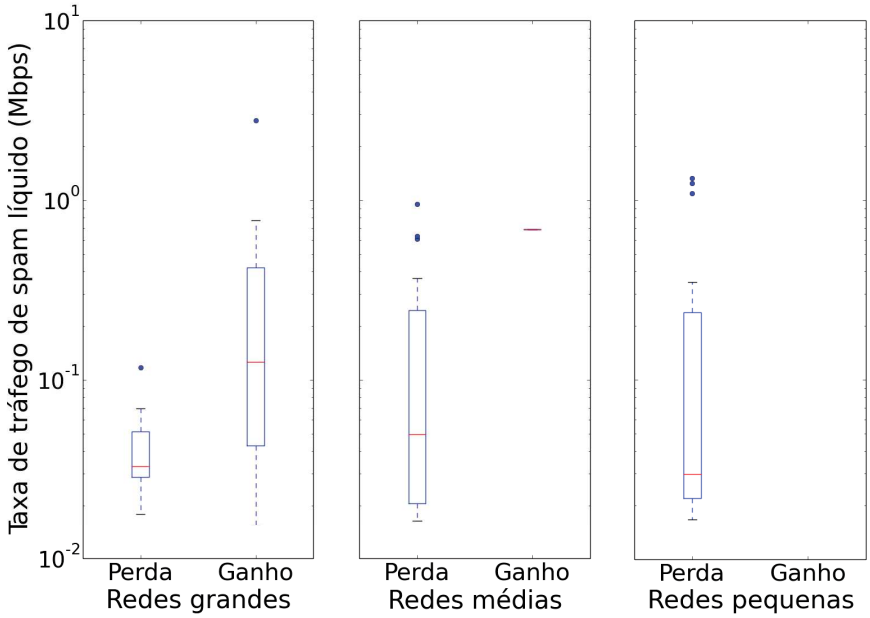

Figura 4.4. Custos associados ao *tráfego líquido de spam*, em função do volume de tráfego, para diferentes classes de redes. Consideramos que redes grandes têm mais de 100 ASes em seus *customer cones*, redes pequenas têm menos de 10 ASes em seus *customer cones* e as redes médias têm *customer cones* de tamanhos entre 10 e 100. Os resultados são qualitativamente similares para pequenas variações nos limiares dos *customer cones*

.

1. Pelo tráfego de saída para seus provedores sempre que não podem encaminhar o tráfego de *spam* para ASes parceiros livre de cobrança. Para os ASes médios presentes na nossa base, isso equivale, em média, a 49,37% do total de custos do tráfego de *spam*. Observamos que o encaminhamento do tráfego de *spam* por ASes parceiros livre de cobrança reduz os custos do tráfego de *spam* em 34,68%, em média, para os ASes na nossa base.

2. Pelo tráfego de entrada recebido de seus provedores. Isso representa 50,73% dos custos para os ASes médios que aparecem nos nossos dados. Notamos que ASes que originam o *spam* têm conectividade pior que ASes que recebem o *spam* (a média do número de provedores somado ao número de parceiros é, respectivamente, 1,38 e 4,31). Isso faz com que o tráfego de *spam* tenha que ir no alto da hierarquia de trânsito da Internet e gere custo para todos os ASes que estão na descida do caminho.

Os ASes médios lucram trocando tráfego de *spam* com seus clientes. Contudo, esses custos podem resultar em valores de *tráfego líquido de spam* negativos quando ASes médios originam ou recebem *spam*, pois o tráfego de *spam* originado e recebido não é encaminhado para nenhum cliente e não geram receita.

O único AS médio que observamos com algum lucro foi a HINETUSA (AS9680, *customer cone* com 24 ASes), que recebe em média 689 kbps (4,3 Gbps) de tráfego de *spam* de seus clientes e encaminha 80,44% deste tráfego através de ASes parceiros. Mais investigações mostraram que todo o *spam* que chega na HINETUSA é oriundo de uma filial em Taiwan (HINET, AS3462).

Pequenos ASes e redes de borda, com *customer cones* menores que dez ASes, pagam pela maior parte do tráfego de *spam*. Esses ASes originam e recebem tráfego de *spam*, resultando em perdas pela troca de tráfego de *spam* com seus provedores. Além dos três *outliers* mostrados na figura 4.4, ASes hospedando os nossos *honeypots* (*customer cones* com 1, 3 e 9 ASes), observamos que 25% dos ASes pagam por uma taxa de *tráfego líquido de spam* superior a 237 Kbps (1.48 Gbps). Esses ASes são sistematicamente onerados pelo tráfego de *spam* e provavelmente estariam dispostos a adotar mecanismos para filtrar as mensagens de *spam* na origem e reduzir esses custos.

4.4 Caracterização das redes que mais enviam spam

Nesta seção investigamos os sistemas autônomos que mais enviam mensagens de *spam* e discutimos as propriedades de cada uma dessas redes. Primeiro mostramos com o gráfico na figura 4.5 que o envio de *spam* não segue uma distribuição uniforme, com a maior parte dos endereços IP (90%) enviando menos de cinco mil mensagens e pouquíssimos (menos de 5%) sendo responsáveis por mais de dez mil mensagens.

Finalmente, quando consideramos a granulariade de AS, evidenciamos que poucas redes são responsáveis pela maior parte do envio de *spam*. Na figura 4.6, por exemplo,

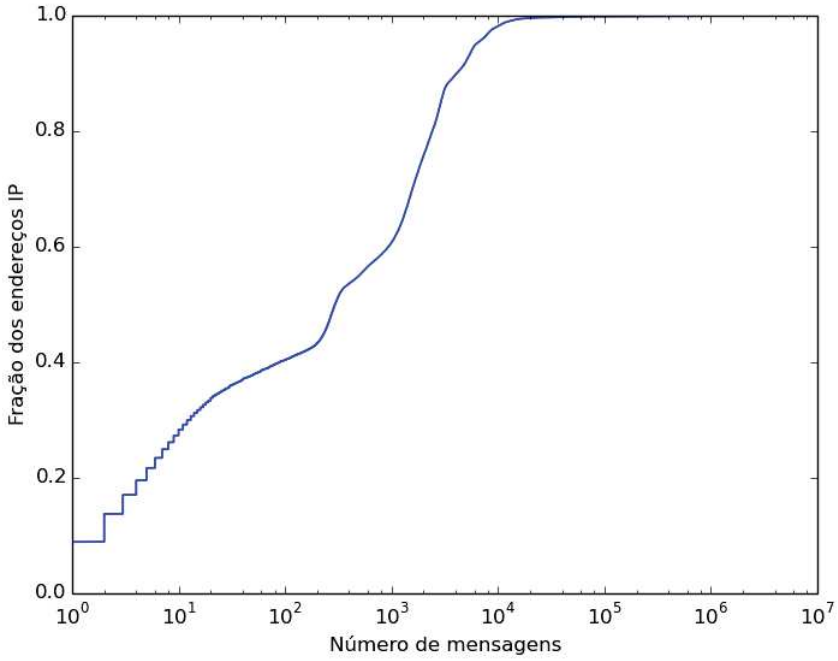

Figura 4.5. CDF do número de mensagens por endereço IP

mostramos que apenas dez ASes (dos 879) são responsáveis por mais de 80% do envio. Note a escala logarítmica no eixo x. Isso reforça a ideia de que a cooperação de apenas algumas redes para filtrar *spam* próximo à origem pode reduzir drasticamente o tráfego de *spam*. O estudo nesta seção é destinado a entender essas dez redes e identificar características que nos permitem separar redes que se beneficiam de redes que são sistematicamente oneradas pelo tráfego de *spam*, i.e., diferenciar entre redes que têm interesse e redes que não se beneficiam da filtragem de *spam*.

A tabela 4.5 lista algumas propriedades das redes que mais enviam *spam* na nossa base. O AS que mais envia *spam* é a HINET (AS3462), mas sabemos que boa parte das mensagens de *spam* são enviadas sem custo através de parceiros até os *honeypots*. Assim, essa rede provavelmente não tem interesse em filtrar as mensagens de *spam*, tornando inviável a maioria das técnicas recentes para filtrar o envio de *spam* na origem. A tabela 4.5 também mostra que a HINET tem mais de 32 mil endereços IP enviando *spam*, cada um deles enviando, em média, apenas 9,18 MB. Essa é uma técnica utilizada para dificultar a identificação dos *spammers* e evitar que os endereços IP caiam em *blacklists*. Os demais ASes menores, com menos de 50 ASes em seus *customer cones*, pagam por 100,00% do tráfego de *spam* enviado por eles. De forma especial, alguns ASes (e.g., CNT, QuadraNet, ROUTIT) têm menos de 4 endereços IP enviando *spam*, sendo os prejuízos ainda maiores, pois recebem de poucos clientes (*spammers*) por todo esse volume de *spam* enviado. Esses ASes têm incentivos para

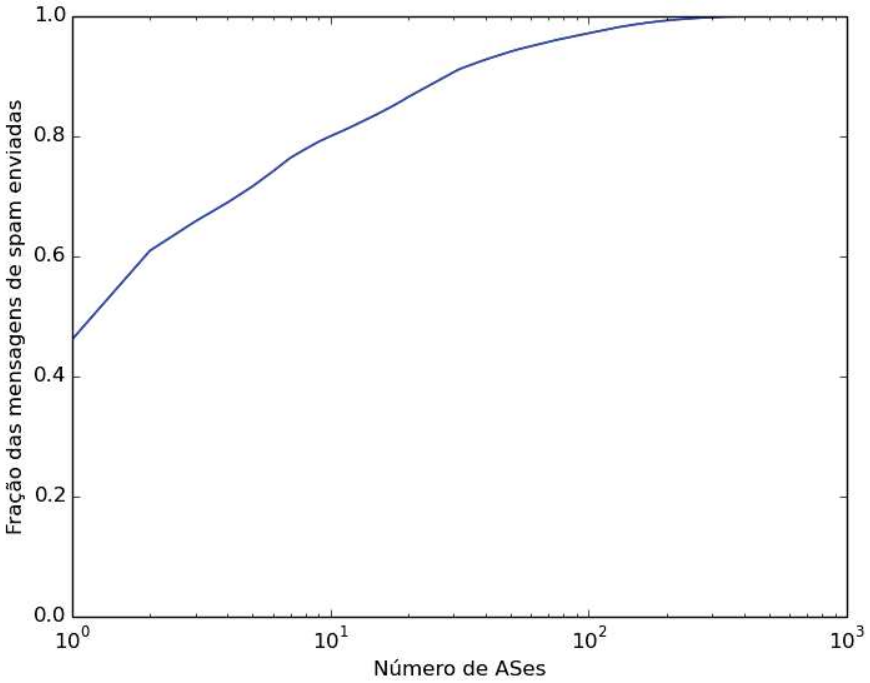

Figura 4.6. Distribuição do envio de *spam* pelos Sistemas Autônomos.

adotar medidas para filtragem de *spam* na origem ou no meio da rede.

Tabela 4.5. ASes responsáveis pela maior parte do tráfego de *spam*

AS	tráfego total (GB)	tráfego pago (%)	customer cone	número de endereços IP
HINET (3462)	293,88	100,00	27	32.755
InfoSphere (2514)	93,94	100,00	13	107
CNT (8615)	31,08	100,00	35	1
Voxel (29791)	20,03	-	16	1
QuadraNet (8100)	17,13	100,00	26	4
ROSTelecom (42610)	15,98	100,00	44	7
ChinaNet (4134)	14,18	11,80	604	18.969
NTT Corp. (4713)	9,26	63,31	577	16
ROUTIT (28685)	7,75	99,99	5	3
Webfusion (20738)	5,89	-	3	7

Uma rede que se destaca é a ChinaNet (AS4134), que 88,20% do tráfego enviado por ela é encaminhado através de parcerias. Isso se deve ao tamanho do seu *customer cone* (604 ASes), que permite a essa rede alcançar um número grande de redes sem a necessidade de um provedor, i.e., sem custo. Essa rede, assim como a HINET, consegue encaminhar boa parte das mensagens de *spam* sem custo, fato que provavelmente

influencia diretamente no número de endereços IP enviando *spam*.

4.5 Amplificação do tráfego de spam

No decorrer do trabalho, mostramos que os custos gerados pelo tráfego de *spam* são aumentados ao atingir servidores SMTP, pois uma cópia da mensagem deve ser enviada para cada domínio distinto que aparece nos destinatários. Nesta seção iremos explorar o problema de amplificação do tráfego e quantificar o aumento do tráfego ao sair dos *honeypots*, independentemente se esse tráfego gera custo para os ASes que hospedam nossos *honeypots*. Para calcular o volume de mensagens do *honeypot* aos destinatários do *spam* supomos que apenas uma cópia da mensagem seria enviada para todos os recipientes em um mesmo servidor de destino, como recomendado no RFC 5321. O tráfego poderia ser ainda maior caso a recomendação do RFC não fosse seguida.

Tabela 4.6. Tráfego de entrada e saída dos ASes que hospedam os *honeypots*

	ID	TRÁFEGO TOTAL (GB)	TRÁFEGO PAGO (%)	TRÁFEGO SEM CUSTO (%)
SPAMMER AO HONEYPOT	AT-01	131,67	99,97	0,03
	BR-01	83,22	100,00	0,00
	NL-01	136,31	98,49	1,51
	US-03	94,47	43,08	56,92
	UY-01	69,47	93,07	6,93
HONEYPOT AO DESTINO	AT-01	301,63	99,99	0,01
	BR-01	323,20	100,00	0,00
	NL-01	113,24	57,22	42,78
	US-03	511,75	15,52	84,48
	UY-01	340,70	85,43	14,57

A tabela 4.6 mostra o tráfego de entrada e saída dos *honeypots*, discriminando o tráfego pago daquele encaminhado livre de cobrança. As redes com poucos ASes em seus *customer cones* (tabela 4.7) pagam tanto pelo *spam* que chega à suas redes quanto pelo tráfego que sai delas. Em contrapartida, redes maiores pagam bem menos devido à parcerias de troca de tráfego livres de cobrança. O AS do *honeypot* US-03, por exemplo, recebe 56,92% do volume de *spam* através de parceiros e consegue encaminhar 84,48% do tráfego de *spam* que sai da sua rede sem custo (depois da amplificação do tráfego, essa rede deixa de pagar por 432,33 GB por causa dessas parcerias de troca de tráfego).

Na tabela 4.7 mostramos a amplificação do tráfego de *spam* que ocorreria caso as mensagens tivessem sido encaminhadas aos servidores de destino pelos *honeypots*. A

Tabela 4.7. Amplificação do tráfego de *spam* ao chegar nos *honeypots*

ID	Amplificação do tráfego	Amplificação do tráfego pago	Tamanho do customer cone
AT-01	2,29x	2,29x	3
BR-01	3,88x	3,88x	1
NL-01	0,83x	0,48x	26
US-03	5,41x	2,08x	82
UY-01	4,90x	4,50x	9

redução do tráfego para o *honeypot* NL-01 mostrado na tabela 4.7 só é possível porque a cobertura das rotas percorridas pelas mensagens de *spam* entre os *spammers* e os *honeypots* (92,26%) é maior que a cobertura das mensagens que seriam enviadas pelos *honeypots* aos servidores de destino (69,53%). O efeito de amplificação seria ainda maior se a cobertura do segundo trecho fosse maior.

A maior amplificação de tráfego acontece no *honeypot* US-03, no qual o tráfego de saída é 5,41 vezes superior ao de entrada. Porém, ao analisar apenas o tráfego que gera custo para essa rede, esse aumento é de apenas 2,08 vezes. Isso acontece porque o AS em que o coletor está hospedado opta por enviar as mensagens através de ASes parceiros sempre que pode (ao receber as mensagens ele não pode escolher) e devido ao tamanho do *customer cone*. Considerando o custo gerado pelo tráfego de *spam* para essas redes, o AS que hospeda o UY-01 é o mais onerado, pagando 4,5 vezes mais para encaminhar as mensagens de *spam* aos servidores de destino. O segundo mais onerado é o AS do *honeypot* BR-01, cujo custo para encaminhar as mensagens de *spam* para os servidores de destino é 388,36% superior se comparado com o custo para receber essas mensagens dos *spammers*. Esses resultados mostram que o impacto causado por filtros de *spam* instalados nos ASes que hospedam os *honeypots* ou que impeçam as mensagens de alcançar os servidores SMTP é muito maior, pois reduzem drasticamente o custo do tráfego gerado para os operadores de rede, em particular, dos ASes que hospedam os servidores SMTP e teriam que pagar por todo o tráfego amplificado.

Capítulo 5

Filtrando o Tráfego de Spam

Neste capítulo utilizamos nossas descobertas para propor um algoritmo que identifica ASes com interesse em filtrar o tráfego de *spam*. Observamos que alguns ASes lucram com o tráfego de *spam* e não teriam interesse em gastar recursos humanos e computacionais para filtrar o tráfego de *spam*. Também notamos que mesmo ASes que pagam pelo tráfego de *spam* podem não ter incentivo econômico em filtrar mensagens de *spam* na descida do caminho (*downstream*), i.e., quando eles poderiam encaminhar o tráfego de *spam* para um de seus clientes. Na figura 3.1, por exemplo, o AS7 estaria disposto a filtrar *spam* vindo do AS9 e destinado ao AS10, a pedido do AS10, pois receberia do AS9 pagamento por esse tráfego e não teria que pagar para o AS3; por outro lado, o AS7 não estaria disposto a filtrar *spam* do AS10 ao AS9, a pedido do AS9, pois o AS7 recebe mais do AS9 do que paga para o AS3. Uma solução prática seria filtrar o tráfego de *spam* no AS que origina o tráfego ou próximo a ele.

Algoritmo 1 Escolher parceiros para a filtragem de spam

Entrada: Mensagens de spam, rotas no nível de AS, relações comerciais entre ASes
Saída: $C[x][y]$: tráfego que x e y podem filtrar para reduzir o custo do *spam*

```
1: for each AS x do
2:     S_in ← conjunto de mensagens que x recebe de provedores
3:     for each AS y no caminho das mensagens em S_in do
4:         if y utiliza um provedor para encaminhar as mensages até x then
5:             C[x][y] ← volume de tráfego de spam entre x e y
6:     S_out ← conjunto de mensagens que x encaminha para provedores
7:     for each AS y que hospeda domínios de destino das mensagens em S_out do
8:         if y recebe mensagens encaminhadas por x de um provedor then
9:             C[x][y] ← C[x][y]+ volume de tráfego de spam entre x e y
```

O algoritmo 1 resume a nossa proposta para identificar possíveis parcerias para filtrar o tráfego de *spam*. Cada AS x na Internet pode coletar as mensagens de *spam*

recebidas de um provedor, i.e., mensagens pelas quais ele paga. O AS x pode, então, utilizar nossa metodologia para identificar quais outros ASes pagam a um provedor para enviar estas mensagens de *spam* e que provavelmente se beneficiariam caso elas fossem filtradas. Assim, o AS x pode comunicar com esses ASes a fim de estabelecer acordos para filtrar as mensagens de *spam*. De forma análoga, cada AS x pode coletar as mensagens de *spam* encaminhadas por ele a um provedor e utilizar nossa metodologia para identificar quais ASes hospedando os domínios de destino pagam para receber essas mensagens. O AS x pode se comunicar com esses ASes e oferecer para filtrar o tráfego de *spam* destinado a eles.

O tráfego de *spam* poderia ser filtrado no nível de pacote, por exemplo, filtrando todo o tráfego de uma fonte (*spammer*) para um destino (servidor SMTP) baseado nos endereços IP, sem a necessidade de inspecionar os pacotes. Uma filtragem seletiva, por outro lado, que consegue distinguir mensagens de *spam* de mensagens legítimas, exige um processamento muito mais complexo no AS intermediário.

Na seção 4.4, por exemplo, discutimos o comportamento da HINET, rede responsável pela maior parte do tráfego de *spam* e que consegue enviar boa parte desse tráfego através de parcerias. Assim, como essa rede não tem interesse em filtrar as mensagens de *spam*, não é possível bloquear o tráfego na origem. Apesar disso, aqueles parceiros utilizados pela HINET, que terão que pagar para encaminhar essas mensagens de *spam* a seus provedores, provavelmente têm interesse em filtrar essas mensagens de *spam* e podem utilizar o algoritmo proposto para encontrar quais ASes hospedando os servidores de destino pagam para receber essas mensagens. Então, o parceiro da HINET que está sendo onerado pode comunicar com os ASes identificados e oferecer para filtrar essas mensagens.

Ainda que o AS parceiro da HINET (que estava sendo onerado) não utilizasse nosso algoritmo, o custo do tráfego de *spam* para essa rede poderia ser reduzido. Para isso, o AS hospedando o domínio de destino precisaria estar utilizando o algoritmo proposto e, assim, verificaria que o AS parceiro da HINET estava sendo onerado por esse tráfego e pediria para o mesmo filtrar as mensagens de *spam* destinadas a ele.

Na figura 5.1, a curva em azul mostra a distribuição da possível economia em relação ao custo do tráfego de *spam* para todos os ASes médios e pequenos que aparecem na nossa base. Nós calculamos a possível economia para cada AS como a fração de tráfego de *spam* trocada com provedores que pode ser filtrada. Mais precisamente, computamos a possível economia para um AS x como sendo a razão entre o custo do tráfego de *spam*, quando todos os ASes aceitam filtrar todas as mensagens de *spam* que geram custos, pelo custo total do tráfego de *spam* sem nenhuma filtragem. A curva mostra que a filtragem, considerando apenas situações em que as redes estão

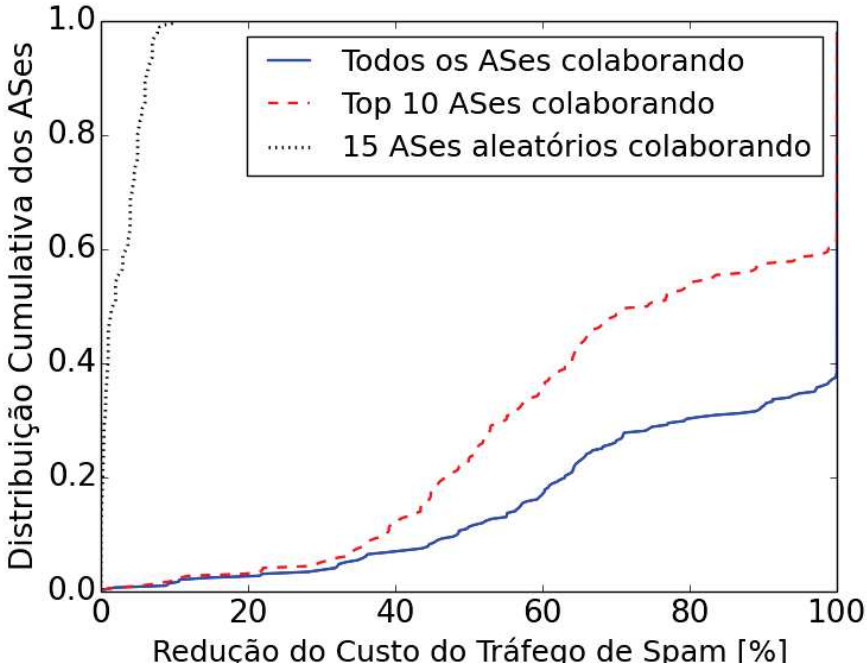

Figura 5.1. Redução do tráfego de *spam* quando o *spam* é filtrado próximo à origem. Nós mostramos uma curva pro cenário quando cada AS coopera com todos os outros, quando cada AS coopera com o dez ASes que geram uma maior redução do tráfego de acordo com nosso algoritmo e quando cada AS coopera com outros quinze ASes escolhidos aleatoriamente.

sendo oneradas, pode mitigar todo o custo do tráfego de *spam* para 60,14% dos ASes e reduzir o custo do tráfego de *spam* no mínimo pela metade para 88,66% dos ASes.

A curva tracejada em vermelho da figura 5.1 mostra a distribuição da redução do custo do tráfego de *spam* quando cada AS estabelece acordos com apenas dez ASes identificados pelo algoritmo. Consideramos que cada AS estabelece acordos com os dez ASes que o levarão a uma maior redução dos custos associados ao tráfego de *spam*, calculado pela nossa metodologia. Depois de escolher um AS para estabelecer um acordo, recalculamos o custo do tráfego de *spam*, i.e., executamos algoritmo 1 novamente, antes de pegar o próximo AS. Notamos que a cooperação de poucos ASes, apenas dez, é suficiente para alcançar uma redução significativa dos custos quando os ASes são escolhidos de forma inteligente. A cooperação com os esses dez ASes pode mitigar todo o custo do tráfego de *spam* para 37,00% dos ASes e reduzir o custo do tráfego de *spam* no mínimo pela metade para 77,06% dos ASes.

Por fim, a curva pontilhada em preto próxima ao eixo y na figura 5.1 mostra a distribuição da redução dos custos esperada quando cada AS x estabelece acordos para filtragem de *spam* com quinze ASes aleatórios (sem utilizar nossa metodologia). Nós

aproximamos a redução de custos esperada como a média da redução para 100 amostras aleatórias de quinze acordos para filtragem de *spam*. A curva mostra que escolher parcerias aleatoriamente não contribui para uma redução significativa dos custos. Isso acontece porque a maioria (90,28%) dos ASes não encaminha *spam* para x ou não têm interesse em filtrar o tráfego de *spam* de x. Em suma, nossos resultados mostram como o custo associado ao tráfego de *spam* pode ser reduzido se houver cooperação entre os ASes e os mesmos utilizarem o algoritmo proposto.

Capítulo 6

Conclusão e Trabalhos Futuros

Neste trabalho, apresentamos uma metodologia para estimar o custo gerado pelo tráfego de *spam* na granularidade de Sistemas Autônomos (ASes). As mensagens de *spam* utilizadas foram coletadas por cinco *honeypots* de baixa interatividade do projeto *SpamPots*, coordenado pelo CERT.br.. Realizamos medições de *traceroute* a partir da plataforma RIPE Atlas para inferir as rotas percorridas por essas mensagens, identificamos os ASes em cada uma das rotas e utilizamos a base de relações entre ASes da CAIDA para inferir o custo do tráfego para cada um dos ASes.

Utilizamos nossa base de dados para caracterizar o custo do tráfego de *spam* atualmente. Mostramos que, em geral, redes maiores lucram com o tráfego de *spam* enquanto redes médias e pequenas pagam por este tráfego. Grandes provedores (e.g., Level3 e NTT Comm.), podem lucrar duas vezes pelo tráfego de *spam*, ao receber tráfego de um cliente e encaminhar a outro. Além disso, discutimos que mesmo ASes que pagam pelo tráfego de *spam*, quando conseguem encaminhar estas mensagens através de clientes, podem não estar interessados em filtrá-las, pois provavelmente pagam menos à seus provedores que os valores cobrados de seus clientes. Finalmente, quantificamos o efeito amplificador que as mensagens de *spam* têm ao alcançar servidores SMTP e como o tráfego de *spam* pode ser reduzido drasticamente se forem instalados filtros para que essas mensages não atinjam tais servidores.

Utilizamos essas descobertas para propor um algoritmo para identificar pares de ASes que provavelmente seriam beneficiados se houvesse uma cooperação na filtragem do tráfego de *spam* próximo à origem. Nosso algoritmo usa apenas dados e informações facilmente disponíveis e pode ser utilizado por qualquer AS ou oferecido como um serviço. Nossas avaliações mostram que o nosso algoritmo pode ajudar a encontrar outros ASes que se beneficiariam e estariam dispostos a cooperar para filtrar o *spam*. Os resultados mostram que utilizar nosso algoritmo na escolha de pares de ASes para

estabeler cooperação na filtragem de *spam* é significativamente melhor que escolher aleatoriamente.

Nossas contribuições são aplicáveis aos atuais esforços na filtragem de *spam* e podem levar à redução do tráfego gerado por esse tipo de atividade. Ainda mais importante, nosso trabalho inicia uma discussão sobre quais redes estão sendo sistematicamente oneradas pelo tráfego de *spam* e serve como incentivo para que haja cooperação por parte desses ASes na filtragem do tráfego de *spam*.

Como trabalhos futuros pretendemos realizar essas análises para outras fontes de tráfego indesejado, e.g., tráfego gerado por Ataques de Negação de Serviço Distribuído (DDoS). Assim, conseguiremos comparar os custos gerados pelo tráfego de *spam* com custos causados por outros tipos de tráfego indesejado e mostrar pontos gerais e específicos do tráfego de *spam*. Além disso, pretendemos criar um serviço de monitoramento constante utilizando as mensagens de *spam* coletadas diariamente, com a finalidade de alertar aqueles ASes que estão tendo os seus custos aumentados e servindo de incentivo para que mais ASes utilizem nosso algoritmo e fiquem motivados à cooperar com a filtragem de *spam* próxima à origem.

Referências Bibliográficas

Amini, L. D.; Shaikh, A. & Schulzrinne, H. G. (2002). Issues with inferring internet topological attributes. Em *ITCom 2002: The Convergence of Information Technologies and Communications*, pp. 80--90. International Society for Optics and Photonics.

Anderson, D. S.; Fleizach, C.; Savage, S. & Voelker, G. M. (2007). Spamscatter: Characterizing Internet Scam Hosting Infrastructure. Em *USENIX Security Symposium*, pp. 10:1--10:14.

Androutsopoulos, I.; Koutsias, J.; Chandrinos, K. V.; Paliouras, G. & Spyropoulos, C. D. (2000). An evaluation of naive bayesian anti-spam filtering. *arXiv preprint cs/0006013*.

Augustin, B.; Krishnamurthy, B. & Willinger, W. (2009). IXPs: Mapped? Em *Proc. IMC*, pp. 336--349.

Chen, K.; Choffnes, D. R.; Potharaju, R.; Chen, Y.; Bustamante, F. E.; Pei, D. & Zhao, Y. (2009). Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes from P2P Users. Em *Proc. ACM CoNEXT*, pp. 217--228.

Dimitropoulos, X.; Hurley, P.; Kind, A. & Stoecklin, M. (2009). On the 95-Percentile Billing Method. Em *Proc. PAM*.

Duan, Z.; Chen, P.; Sanchez, F.; Dong, Y.; Stephenson, M. & Barker, J. M. (2012). Detecting Spam Zombies by Monitoring Outgoing Messages. *IEEE Trans. Dependable Secur. Comput.*, 9(2):198--210.

Fazzion, E.; Las-Casas, P. H. B.; Fonseca, O.; Guedes, D.; Jr., W. M.; Hoepers, C.; Steding-Jessen, K. & Chaves, M. H. P. (2014). Spambands: Uma metodologia para identificação de fontes de spam agindo sob uma coordenação. Em *Brazilian Symposium on Information Security and Computer Systems (SBSeg) (In Portuguese)*. SBC.

Fonseca, O.; Fazzion, E.; Cunha, Í.; Las-Casas, P. H. B.; Guedes, D.; Meira Jr, W.; Hoepers, C.; Steding-Jessen, K. & Chaves, M. H. (2015). Uma Análise do Custo do Tráfego de Spam para Operadores de Rede. Em *Anais do simpósio brasileiro de redes de computadores e sistemas distribuídos (SBRC)*. SBC.

Fonseca, O.; Fazzion, E.; Cunha, Í.; Las-Casas, P. H. B.; Guedes, D.; Meira Jr, W.; Hoepers, C.; Steding-Jessen, K. & Chaves, M. H. (2016). Measuring, Characterizing, and Avoiding Spam Traffic Costs. Em *IEEE Internet Computing*. (Aguardando publicação).

Fonseca, O.; Las-Casas, P. H. B.; Fazzion, E.; Guedes, D.; Jr., W. M.; Hoepers, C.; Steding-Jessen, K. & Chaves, M. H. P. (2014). Vizinhanças ou condomínios: uma análise da origem de spams com base na organização de sistemas autônomos. Em *Anais do simpósio brasileiro de redes de computadores e sistemas distribuídos (SBRC)*. SBC.

Gao, L. (2001). On Inferring Autonomous System Relationships in the Internet. *IEEE/ACM Trans. Netw.*, 9(6):733--745.

Giotsas, V.; Luckie, M.; Huffaker, B. & kc claffy (2014). Inferring Complex AS Relationships. Em *Proc. IMC*, pp. 23--30.

Gomes, L. H.; Almeida, R. B.; Bettencourt, L. M. A.; Almeida, V. & Almeida, J. M. (2005). Comparative Graph Theoretical Characterization of Networks of Spam and Legitimate Email. Em *Proceedings of the Second Conference on Email and Anti-Spam - CEAS 2005*, Stanford, CA, USA. CEAS.

Gomes, L. H.; Cazita, C.; Almeida, J. M.; Almeida, V. & Meira, W. (2007). Workload models of spam and legitimate e-mails. *Performance Evaluation*, 64(7):690--714.

Gomes, L. H.; Cazita, C.; Almeida, J. M.; Almeida, V. & Meira Jr, W. (2004). Characterizing a spam traffic. Em *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, pp. 356--369. ACM.

Goodman, J.; Cormack, G. V. & Heckerman, D. (2007). Spam and the ongoing battle for the inbox. *Communications of the ACM*, 50(2):24--33.

Hao, S.; Syed, N. A.; Feamster, N.; Gray, A. G. & Krasser, S. (2009). Detecting spammers with snare: Spatio-temporal network-level automatic reputation engine. Em *USENIX Security Symposium*, volume 9.

He, Y.; Faloutsos, M.; Krishnamurthy, S. & Huffaker, B. (2005). On Routing Asymmetry in the Internet. Em *Proc. IEEE GLOBECOM*.

Kanich, C.; Kreibich, C.; Levchenko, K.; Enright, B.; Voelker, G. M.; Paxson, V. & Savage, S. (2008). Spamalytics: An empirical analysis of spam marketing conversion. Em *Proceedings of the 15th ACM conference on Computer and communications security*, pp. 3--14. ACM.

Kim, J. & Choi, H. (2008). Spam traffic characterization. Em *Technical Conference on Circuits/Systems, Computers and Communications*.

Konte, M. & Feamster, N. (2011). Wide-area Routing Dynamics of Malicious Networks. Em *Proc. ACM SIGCOMM*.

Konte, M.; Perdisci, R. & Feamster, N. (2015). Aswatch: An as reputation system to expose bulletproof hosting ases. *SIGCOMM Comput. Commun. Rev.*, 45(5):625--638.

Las-Casas, P. H. B.; Guedes, D.; Almeida, J. M.; Ziviani, A. & Marques-Neto, H. T. (2013a). SpaDeS: Detecting Spammers at the Source Network. *Computer Networks*, 57(2):526--539.

Las-Casas, P. H. B.; Guedes, D.; Jr., W. M.; Hoepers, C.; Steding-Jessen, K.; Chaves, M. H. P.; Fonseca, O.; Fazzion, E. & Moreira, R. E. A. (2013b). Análise do tráfego de spam coletado ao redor do mundo. Em *Anais do simpósio brasileiro de redes de computadores e sistemas distribuídos (SBRC)*. SBC.

Levchenko, K.; Pitsillidis, A.; Chachra, N.; Enright, B.; Félegyházi, M.; Grier, C.; Halvorson, T.; Kanich, C.; Kreibich, C.; Liu, H. et al. (2011). Click trajectories: End-to-end analysis of the spam value chain. Em *Security and Privacy (SP), 2011 IEEE Symposium on*, pp. 431--446. IEEE.

Luckie, M.; Huffaker, B.; Claffy, K.; Dhamdhere, A. & Giotsas, V. (2013). AS Relationships, Customer Cones, and Validation. Em *Proc. IMC*, pp. 243--256.

Madhyastha, H.; Isdal, T.; Piatek, M.; Dixon, C.; Anderson, T.; Krishnamurthy, A. & Venkataramani, A. (2006). iPlane: an Information Plane for Distributed Services. Em *Proc. USENIX OSDI*, pp. 367--380.

Mao, Z. M.; Rexford, J.; Wang, J. & Katz, R. H. (2003). Towards an Accurate AS-level Traceroute Tool. Em *Proc. ACM SIGCOMM*.

McCoy, D.; Dharmdasani, H.; Kreibich, C.; Voelker, G. M. & Savage, S. (2012). Priceless: The role of payments in abuse-advertised goods. Em *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 845--856. ACM.

Meyer, D. et al. (2005). The University of Oregon Routeviews Project. http://www.routeviews.org.

Moreira Moura, G. C.; Sadre, R. & Pras, A. (2011). Internet bad neighborhoods: the spam case. Em Festor, O. & Lupu, E., editores, *7th International Conference on Network and Services Management (CNSM 2011), Paris, France*, pp. 1--8, USA. IEEE Communications Society.

Newman, M. E. J.; Forrest, S. & Balthrop, J. (2002). Email Networks and the Spread of Computer Viruses. *Phys. Rev. E*, 66(3):035101.

Orman, H. (2013). The Compleat Story of Phish. *IEEE Internet Computing*, 17(1):87--91.

Ramachandran, A.; Dasgupta, A.; Feamster, N. & Weinberger, K. (2011). Spam or ham?: characterizing and detecting fraudulent not spam reports in web mail systems. Em *Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference*, pp. 210--219. ACM.

Ramachandran, A. & Feamster, N. (2006). Understanding the Network-level Behavior of Spammers. Em *Proc. ACM SIGCOMM*, pp. 291--302.

Ramachandran, A.; Feamster, N. & Vempala, S. (2007). Filtering spam with behavioral blacklisting. Em *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 342--351. ACM.

Rao, J. M. & Reiley, D. H. (2012). The Economics of Spam. *The Journal of Economic Perspectives*, 26(3):87--110.

RIPE, N. (2005). RIPE Routing Information Service. http://www.ripe.net/data-tools/stats/ris.

Sahami, M.; Dumais, S.; Heckerman, D. & Horvitz, E. (1998). A bayesian approach to filtering junk e-mail. Em *Learning for Text Categorization: Papers from the 1998 workshop*, volume 62, pp. 98--105.

Sipior, J. C.; Ward, B. T. & Bonner, P. G. (2004). Should Spam Be on the Menu? *Communications of the ACM*, 47(6):59--63.

Stanojevic, R.; Laoutaris, N. & Rodriguez, P. (2010). On Economic Heavy Hitters: Shapley Value Analysis of 95th-percentile Pricing. Em *Proc. IMC*.

Steding-Jessen, K.; Vijaykumar, N. L. & Montes, A. (2008). Using low-interaction honeypots to study the abuse of open proxies to send spam. *INFOCOMP Journal of Computer Science*, 7(1):44--52.

Subramanian, L.; Agarwal, S.; Rexford, J. & Katz, Y. H. (2002). Characterizing the Internet Hierarchy from Multiple Vantage Points. Em *Proc. IEEE INFOCOM*.

Symantec (2014). Internet Security Threat Report. 19.

Valancius, V.; Lumezanu, C.; Feamster, N.; Johari, R. & Vazirani, V. V. (2011). How Many Tiers? Pricing in the Internet Transit Market. Em *Proc. ACM SIGCOMM*.

van Wanrooij, W. & Pras, A. (2010). Filtering spam from bad neighborhoods. *International Journal of Network Management*, 20(6):433--444.

Venkataraman, S.; Sen, S.; Spatscheck, O.; Haffner, P. & Song, D. (2007). Exploiting network structure for proactive spam mitigation. Em *Usenix Security*.

Xia, J. & Gao, L. (2004). On the evaluation of as relationship inferences [internet reachability/traffic flow applications]. Em *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, volume 3, pp. 1373--1377. IEEE.

Anexo A

Análises complementares

A.1 Top 10 ASes que mais pagam/recebem pelo tráfego de spam

Tabela A.1. ASes que mais pagam/recebem nas rotas do *spammer* ao *honeypot*

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
HiNet, TW (3462)	293,8	HinetUSA, TW (9680)	265,8
AS *Honeypot* NL-01	134,2	Level 3, US (3356)	155,0
AS *Honeypot* AT-01	131,6	TWGATE-AP, TW (9505)	93,9
InfoSphere NTT PC, JP (2514)	93,9	NORDUNET, NO (2603)	86,8
AS *Honeypot* BR-01	83,2	Embratel, BR (4230)	83,2
Embratel, BR (4230)	82,0	TELE2, SE (1257)	74,5
Tele2, AT (8437)	74,5	Tele2, AT (8437)	74,5
AS *Honeypot* UY-01	64,6	PCCW Global, US (3491)	73,6
Uninet S.A., MX (28513)	56,4	Wholesale Services, ES (12956)	64,7
NextLayer, AT (1764)	54,4	NextLayer, AT (1764)	56,8

Tabela A.2. ASes que mais pagam/recebem nas rotas do *honeypot* aos servidores de destino

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* BR-01	323,1	Level 3, US (3356)	750,76
AS *Honeypot* AT-01	301,6	Embratel, BR (4230)	323,1
AS *Honeypot* UY-01	291,0	RETN Limited, UA (9002)	313,1
MailRu, RU (47764)	206,4	NextLayer, AT (1764)	301,6
RETN Limited, UA (9002)	169,4	Cogent, US (174)	166,6
Yandex LLC, RU (13238)	114,1	NTT America, US (2914)	138,9
Embratel, BR (4230)	105,3	Tinet Spa, DE (3257)	118,5
Rambler LLC, RU (24638)	89,8	RASCOM, RU (20764)	88,8
ROSTelecom, RU (12389)	89,5	ROSTelecom, RU (12389)	81,3
RASCOM, RU (20764)	87,2	NORDUNET, NO (2603)	64,4

A.2 Soma do custo do tráfego de spam

Tabela A.3. Soma do custo gerado pelo tráfego de *spam* separado por *honeypot*

ID	Spammer ao *honeypot* (GB)	*Honeypot* aos servidores de destino	CC Size
AT-01	441,7	485,7	3
BR-01	309,7	723,8	1
NL-01	268,4	98,7	26
US-03	200,9	881,4	82
UY-01	159,5	795,2	9
Total	1.380,4	1.985,0	0

A.3 Custo para os ASes dos honeypots

Tabela A.4. Custo gerado para os ASes que hospedam os *honeypots*

ID	Spammer ao *honeypot* (GB)	*Honeypot* aos servidores de destino
AT-01	131,6	301,6
BR-01	83,0	323,1
NL-01	134,2	64,8
US-03	40,6	79,3
UY-01	64,6	291,0

A.4 Mapa de relações para os outros honeypots

Nesta seção estão presentes os grafos de custo dos ASes não mencionados no capítulo 4.

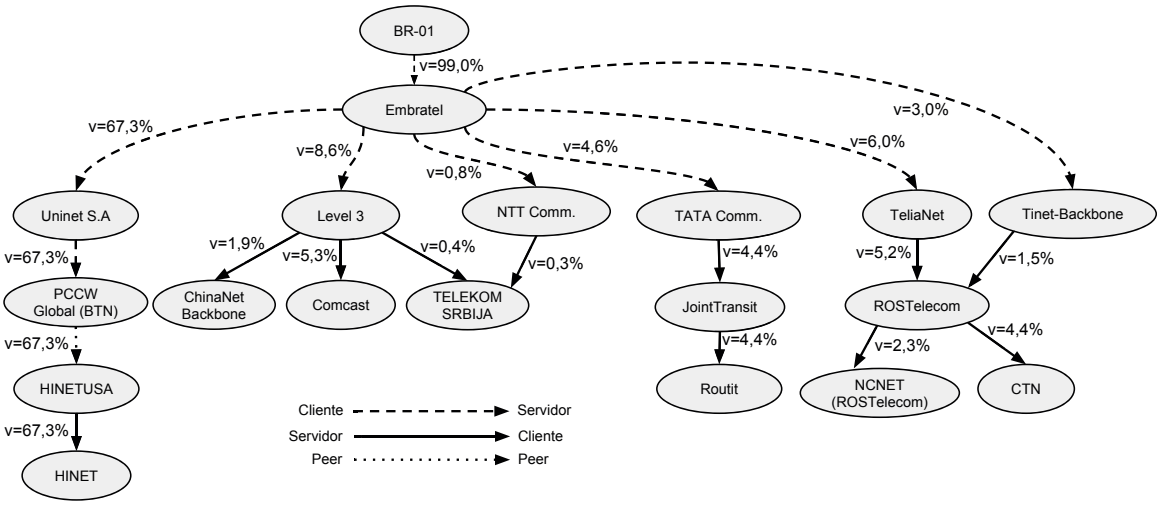

Figura A.1. Mapa dos ASes mais utilizados entre as máquinas que enviam *spam* e o *honeypot*

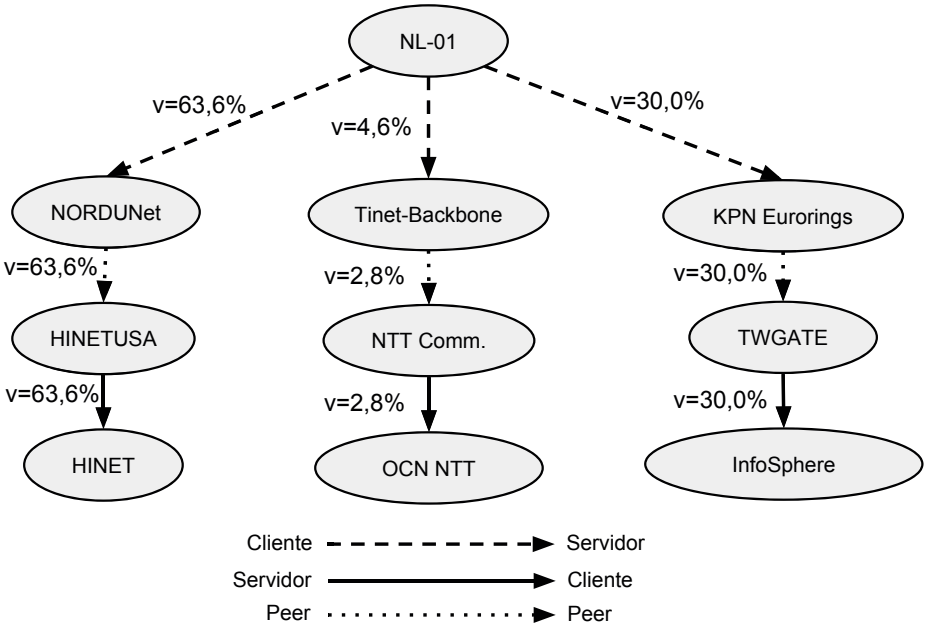

Figura A.2. Mapa dos ASes mais utilizados entre as máquinas que enviam *spam* e o *honeypot*

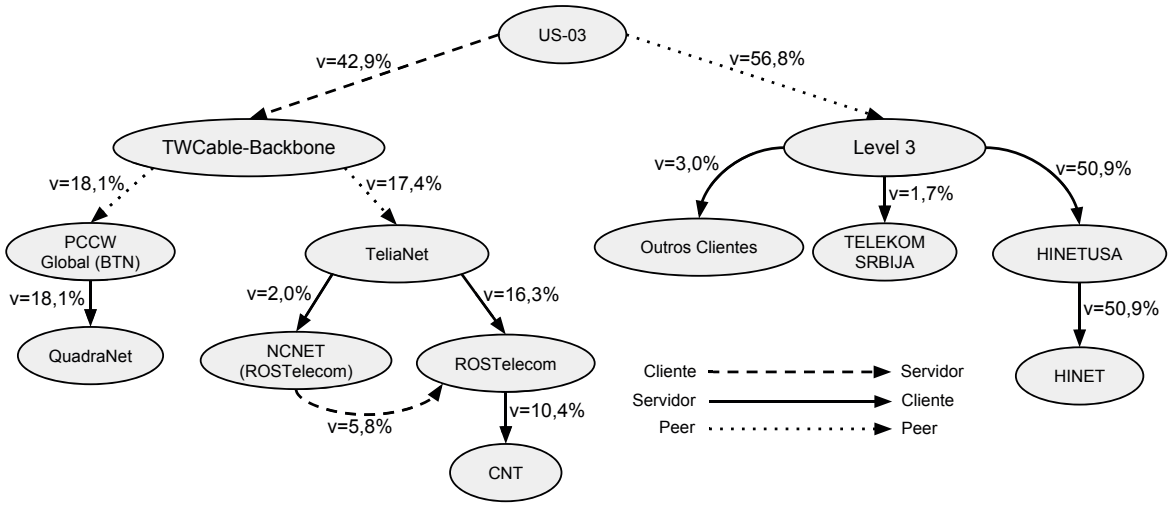

Figura A.3. Mapa dos ASes mais utilizados entre as máquinas que enviam *spam* e o *honeypot*

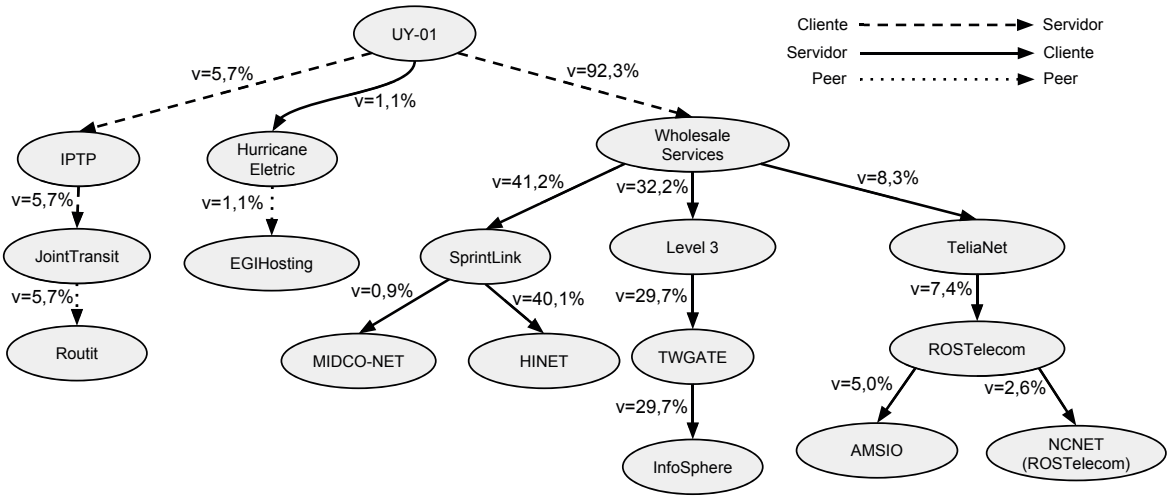

Figura A.4. Mapa dos ASes mais utilizados entre as máquinas que enviam *spam* e o *honeypot*

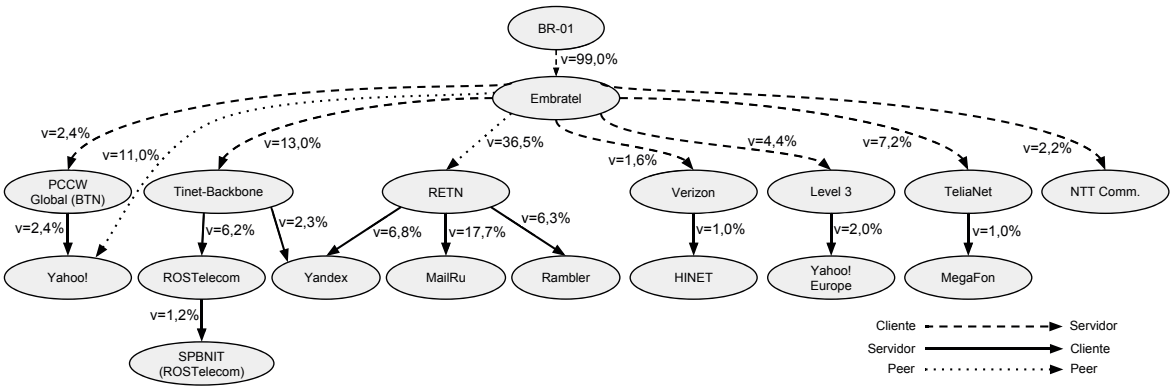

Figura A.5. Mapa dos ASes mais utilizados entre o *honeypot* e os domínios de destino

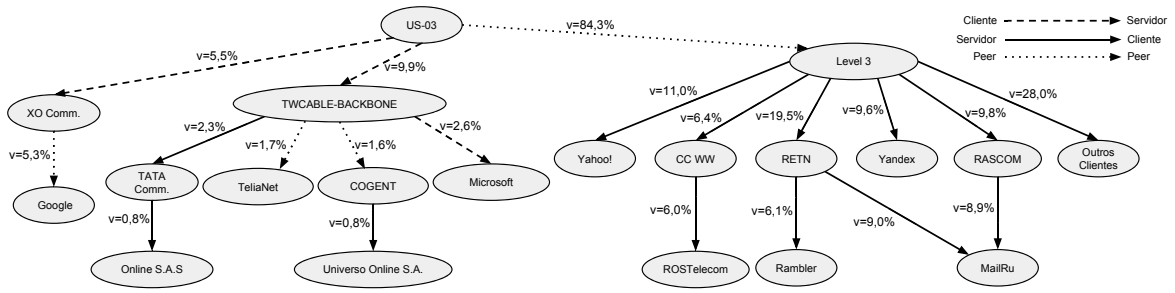

Figura A.6. Mapa dos ASes mais utilizados entre o *honeypot* e os domínios de destino

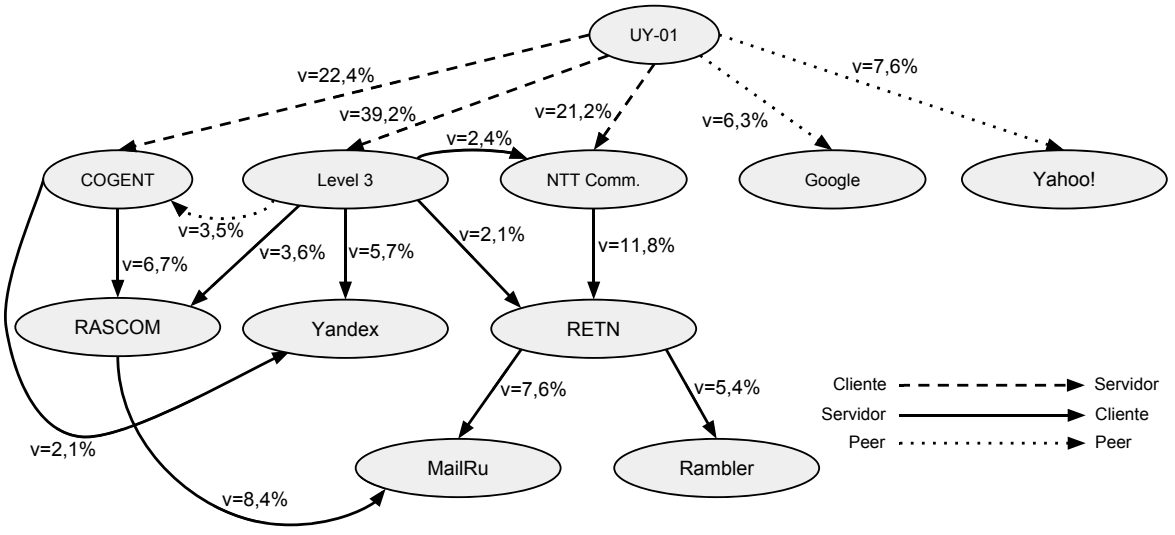

Figura A.7. Mapa dos ASes mais utilizados entre o *honeypot* e os domínios de destino