Uma Análise do Custo do Tráfego de *Spam* para Operadores de Rede

Osvaldo Fonseca[1]*, Elverton Fazzion[1]*, Ítalo Cunha[1], Pedro Henrique B. Las-Casas[1], Dorgival Guedes[1], Wagner Meira Jr.[1], Cristine Hoepers[2], Klaus Steding-Jessen[2], Marcelo H. P. Chaves[2]

[1] Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

[2]CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
NIC.br - Núcleo de Informação e Coordenação do Ponto BR

{osvaldo.morais,elverton,cunha,pedro.lascasas,dorgival,meira}@dcc.ufmg.br

{cristine,jessen,mhp}@cert.br

Abstract. *Spam messages are used to disseminate malware, make phishing attacks, and advertise illegal products. Spam generates costs to users, e.g., victims of phishing, and to network administrators, e.g., who provision and pay for the traffic. Recent proposals aim to identify and filter spam messages at the origin, restraining message propagation and reducing wasted bandwidth on the route from the spammer to the destination. In this work we analyze spam traffic costs for network operators. We measure the routes traversed by real spam messages colected at five honeypots, and estimate spam traffic costs according to the business relationships between networks traversed on each route. We show that stub networks are systematically encumbered by high spam traffic costs but can cooperate to filter up to 70% of spam messages at the origin. Our results also indicate that transit networks that send a lot of spam may employ traffic engineering to reduce their transit costs.*

Resumo. *Mensagens de* spam *são utilizadas para propagação de* malware*, ataques de* phishing *e venda ilegal de produtos. O* spam *gera custos para usuários, e.g., vítimas de* phishing*, e para operadores de rede, e.g., que pagam pela transferência do tráfego. Propostas recentes visam identificar e filtrar mensagens de* spam *na origem, reduzindo o alcance das mensagens e evitando desperdício de banda de rede na rota entre a origem e o destino. Neste trabalho fazemos uma análise do custo do tráfego de* spam *para operadores de rede. Medimos rotas trafegadas por mensagens de* spam *reais coletadas em cinco* honeypots *e estimamos o custo do tráfego de* spam *de acordo com as relações comerciais entre as redes que compõem cada rota. Nossos resultados mostram que algumas redes são sistematicamente oneradas pelo tráfego de* spam *mas que podem cooperar para filtrar até 70% das mensagens de* spam *na origem. Por último, mostramos indícios de que redes que enviam muito* spam *utilizam mecanismos de engenharia de tráfego para reduzir o custo do tráfego.*

*Osvaldo Fonseca e Elverton Fazzion contribuiram de forma equivalente para este trabalho.

1. Introdução

Mensagens de *spam*, e-mails não solicitados enviados para uma grande quantidade de destinatários, estão frequentemente associadas a atividades ilegais. Apesar da maior parte das mensagens de *spam* distribuírem propaganda de produtos ou serviços, *spam* também é utilizado para atrair usuários a réplicas falsas de serviços reais (*phishing*) [Orman 2013] ou propagação de programas maliciosos (*malware*) [Newman et al. 2002]. Mensagens de *spam* corresponderam a 90% do tráfego de mensagens de correio eletrônico em 2013, gerando aproximadamente 216 TB de volume diário [Symantec 2014].

A batalha contra os *spammers* se trava em diversas frentes. Nos últimos anos, muitos trabalhos têm focado em combater o *spam* na origem, de forma a evitar que essas mensagens trafeguem pela Internet da origem até o destino consumindo banda de rede [Las-Casas et al. 2013]. Existem trabalhos na literatura que mostram que o tráfego de *spam* gera um alto custo para a Internet [Sipior et al. 2004, Rao and Reiley 2012]. Entretanto, estes trabalhos consideram apenas o custo agregado e não uma granularidade menor para identificar quais redes são oneradas pelo tráfego de *spam*.

Um Sistema Autônomo (AS) na Internet é uma entidade registrada junto às autoridades da Internet, e.g., ARIN e LACNIC, como operadora de recursos de rede conectados à Internet, como roteadores, enlaces, computadores e faixas de endereços IP. ASes estabelecem relações comerciais com outros ASes, frequentemente envolvendo pagamento por serviços ou por conectividade global. Envio e recebimento de mensagens de *spam* pode resultar em custos diretos para ASes que pagam por tráfego.

Neste trabalho avaliamos o custo do tráfego de *spam*, em bytes, para operadores de rede na granularidade de ASes. Propomos uma abordagem que permite entender quais ASes estão sendo onerados ou beneficiados pelo tráfego de *spam* (seção 2). O primeiro desafio é obter uma amostra representativa do tráfego de *spam* na Internet. Nossa análise é baseada em 78,5 milhões de mensagens de *spam* reais coletadas por *honeypots* instalados em cinco redes em quatro países distintos. O segundo desafio é estimar as rotas trafegadas pelas mensagens de *spam*. Realizamos *traceroutes* de diversos pontos na Internet e utilizamos técnicas de mapeamento de endereços IP em ASes [Chen et al. 2009] para inferir a sequência de ASes nas rotas trafegadas pelas mensagens de *spam*. O terceiro desafio é inferir as relações comerciais entre ASes e a direção do fluxo monetário incorrido pelo tráfego de *spam*. Como os contratos de custos entre ASes são privados, o custo monetário é impossível de obter. Desta forma, utilizamos as relações entre ASes e o tráfego de *spam* em nossa análise. Estas relações foram obtidas de bases dados públicas [Luckie et al. 2013, Giotsas et al. 2014]. Combinando estas diversas fontes de dados conseguimos inferir quanto tráfego de *spam* trafega entre pares de ASes e estimar o custo para cada AS.

Nossos resultados têm aplicações práticas diretas. Identificamos quais ASes são onerados e têm incentivos para filtrar tráfego de *spam* e quais ASes se beneficiam do tráfego de *spam*. Este resultado facilita a cooperação entre redes oneradas para combater o *spam*, e.g., através da instalação de filtros distribuídos de *spam* na origem. Em particular, redes de borda são as mais oneradas e as que têm maior incentivo para a implantação de mecanismos para filtragem e bloqueio de *spam* na origem. Além disso, mostramos que, se algumas redes cooperassem, poder-se-ia filtrar até 70% das mensagens de *spam* na origem. Ainda mais, mostramos o impacto no volume de tráfego que as mensagem de *spam* podem ter se encaminhadas por servidores SMTP e como a instalação de filtros que impeçam esse fato poderiam reduzir drasticamente o tráfego. Por fim, nossos resultados também motivam novas técnicas para identificação do tráfego de *spam*, e.g., detectar engenharia de tráfego com objetivo de amortizar rajadas e custo do tráfego.

2. Conjuntos de dados

Nesta seção explicamos como capturamos mensagens reais de *spam* representativas do tráfego global (seção 2.1) e como inferimos as rotas trafegadas pelas mensagens na Internet utilizando medições distribuídas a bases de dados diversas (seção 2.2).

2.1. Coleta de mensagens de *spam*

As mensagens de *spam* que utilizamos em nossa análise foram coletadas de cinco *honeypots* instalados em diferentes países, dois no Brasil, um na Holanda, um nos Estados Unidos e um no Uruguai, em redes de diferentes características. *Honeypots* são máquinas que simulam servidores vulneráveis para atrair *spammers*. Os *honeypots* são configurados para *simular proxies* HTTP e SOCKS bem como *relays* SMTP abertos. Quando um *spammer* se conecta ao servidor SMTP de um *honeypot*, ele é levado a crer que está interagindo com um servidor SMTP operando como um *relay* aberto.[1] Quando uma máquina se conecta a um *honeypot* através dos protocolos HTTP ou SOCKS, é levada a crer que é capaz de estabelecer conexões com outros servidores SMTP na rede. Estes serviços são frequentemente utilizados para o envio de spam. Além disso, como esses protocolos são orientados a conexão, é improvável a ocorrência de IP spoofing, que só seria possível se feito ao longo da rota de retorno dos pacotes e durante toda a duração da conexão.

Como os *honeypots* não prestam serviço para nenhuma rede e não são anunciados publicamente, assumimos que toda a interação com os *honeypots* provém de *spammers*. Toda interação com os *honeypots* é registrada e as mensagens de *spam* são armazenadas localmente. Nenhuma mensagem de *spam* é efetivamente entregue ao seu destino nem conexões SMTP via proxies efetivamente estabelecidas—exceto para mensagens classificadas como mensagens de teste segundo regras pré-definidas.[2] Periodicamente, ao longo de cada dia, todo o spam armazenado nos *honeypots* é copiado para os servidores centrais do projeto. A distribuição dos *honeypots* em diferentes países e diferentes redes (e.g., redes acadêmicas e comerciais no Brasil) visa obter uma visão geral do tráfego de *spam* na Internet. Neste trabalho analisamos mensagens coletadas entre 01/08/2014 e 31/08/2014. A tabela 1 oferece uma visão geral dos dados coletados. Um detalhe importante sobre os dados utilizados no trabalho é que eles são de natureza sensível e não podem ser publicados, por oferecerem diversas formas para identificação dos honeypots e conterem endereços válidos de usuários que seriam alvo de spam. A sanitização dessas informações reduziria grandemente o interesse dos dados.

Neste período coletamos 78,5 milhões de mensagens, provenientes de 722 ASes de origem distintos em 122 países. O número de endereços IP que utilizam o protocolo SMTP é maior (98,50% do total) do que daqueles que utilizam HTTP/SOCKS e enviam 56,01% das mensagens de *spam*. Estas observações seguem padrões observados em trabalhos anteriores, cujos endereços IP que utilizam SMTP são típicos de participantes em

[1] Servidores SMTP de *relay* aberto encaminham mensagens de e-mail recebidas para outros servidores.

[2] Por exemplo, verificando presença de texto específico no assunto ou corpo da mensagem.

Tabela 1. Visão geral da base de *spam*.

MÉTRICA	HTTP/SOCKS	SMTP	TOTAL
Mensagens (milhões)	34,54 (44%)	43,99 (56%)	78,53
Endereços IP de origem	491 (2%)	32 336 (98%)	32 826
Prefixos de rede de origem	264 (18%)	1 243 (83%)	1 492
Sistemas autônomos de origem	110 (15%)	653 (90%)	722
Código de países (IPs de origem)	36 (30%)	118 (97%)	122
Volume de Tráfego (GB)	129,34 (27%)	341,33 (73%)	470,68

Tabela 2. Quantidade de *spam* por *honeypot*.

ID	MILHÕES DE MENSAGENS	ENDEREÇOS IP DE ORIGEM	ASES DE ORIGEM	ASES NÃO COBERTOS	VOLUME (GB)
BR-01	12,25 (16%)	31 084 (95%)	552 (76%)	328 (59%)	91,33 (19%)
BR-02	19,51 (25%)	24 317 (74%)	178 (25%)	82 (46%)	85,01 (18%)
NL-01	22,99 (29%)	23 264 (71%)	245 (34%)	132 (54%)	119,60 (25%)
UY-01	13,52 (17%)	24 046 (73%)	500 (69%)	300 (60%)	73,34 (16%)
US-03	10,24 (13%)	26 346 (80%)	483 (67%)	296 (61%)	101,59 (22%)

botnets, que têm baixo volume de mensagens por IP de origem. Os poucos endereços IP que utilizam HTTP/SOCKS (1,50% do total) têm volume muito maior de mensagens, típico de servidores de *spam* dedicados.

A tabela 2 mostra a quantidade de mensagens, o número de IPs de origem distintos, o número de ASes de origem e o volume das mensagens recebidas observados em cada *honeypot*. Note que existe sobreposição de IPs entre *honeypots*, o que indica que *spammers* conectam-se a mais de um *honeypot*.

2.2. Inferência das rotas trafegadas pelo *spam*

Para inferir as rotas percorridas pelas mensagens de *spam*, primeiro coletamos medições utilizando *traceroute* e depois mapeamos os endereços IP nos traceroutes em sistemas autônomos (ASes).

Usamos as plataformas RIPE Atlas e PlanetLab para medir as rotas que seriam trafegadas pelas mensagens de *spam* dos *honeypots* até seus destinos, caso as mensagens tivessem sido entregues. Estas plataformas possuem monitores em milhares de redes ao redor do globo, inclusive nas redes dos *honeypots*. Como os ASes onde os *honeypots* estão hospedados são ASes locais e de ponta, os dispositivos RIPE Atlas e PlanetLab provavelmente usam a mesma rota dos *honeypots* até os *spammers* [Mühlbauer et al. 2007]. Durante nossas medições observamos que 29% dos domínios de destino não puderam ser resolvidos ou não possuem servidor de e-mail configurado no DNS (i.e., o domínio não configura registro MX no DNS), o que impossibilita realizar uma medição *traceroute* para o servidor de e-mail. Isto pode acontecer para destinatários gerados (semi-)automaticamente. Como um *relay* não encaminharia mensagens de e-mail nesse caso, ignoramos estes domínios.

Para medir as rotas trafegadas pelas mensagens de *spam* dos *spammers* até os *honeypots*, seria necessário ter acesso a dispositivos próximos aos *spammers*. Essa abordagem não é prática pois as mensagens de *spam* são enviadas de 722 ASes distintos, 58,12% deles não cobertos por nós PlanetLab ou RIPE Atlas. O número de ASes não cobertos, por *honeypot*, pode ser visto na tabela 2. Para contornar este problema realizamos medições dos *honeypots* até os *spammers*, utilizando as plataformas RIPE Atlas e PlanetLab, e assumimos que a rota dos *spammers* até os *honeypots* é simétrica. Uma limitação desta abordagem é que rotas na Internet são frequentemente assimétricas [He et al. 2005].

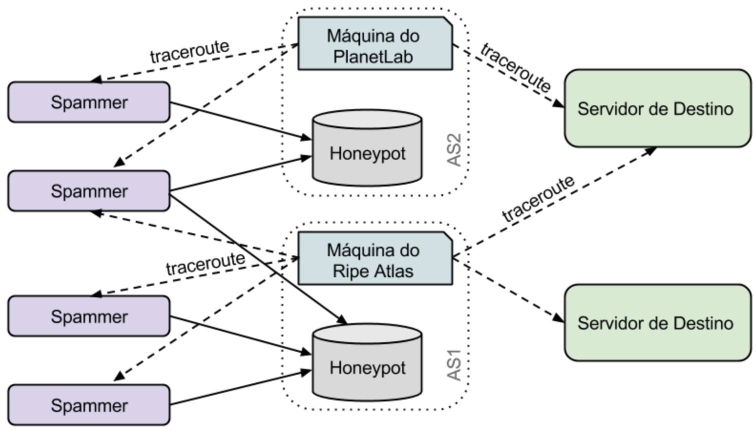

Figura 1. Arquitetura utilizada na coleta das medições de *traceroute*

A figura 1 ilustra a plataforma que implantamos para coletar medições de *traceroute*. A figura ilustra que usamos coletores PlanetLab e RIPE Atlas distintos dentro do AS de cada *honeypot* bem como a sobreposição de *spammers* e destinatários entre os *honeypots*. Por último, a direção das arestas pontilhadas mostra o sentido das medições *traceroute* e as arestas sólidas mostram o sentido das mensagens de *spam*.

Como nosso estudo é baseado nas relações entre ASes, precisamos mapear endereços IP obtidos nas medições com *traceroute* em seus respectivos ASes. Utilizamos as bases de mapeamento de endereço IP em número de AS do iPlane [Madhyastha et al. 2006] e do Team Cymru.[3] Após aplicar as bases de dados para converter endereços IP em ASes, nós substituímos sequências do mesmo AS por uma única ocorrência e aplicamos heurísticas propostas por [Chen et al. 2009] para tratar erros de mapeamento causados por endereços IP que não estão nas bases de dados. Em particular, se um endereço IP x não foi mapeado mas está cercado por endereços IP mapeados para um mesmo AS_1, e.g., $[\cdots, \mathrm{AS}_1, x, \mathrm{AS}_1, \cdots]$, então substituímos x por AS_1. A fração de rotas em nosso conjunto de dados com erros de mapeamento entre sistemas autônomos distintos, e.g., $[\cdots, \mathrm{AS}_1, x, \mathrm{AS}_2, \cdots]$, varia de 2 a 25% dependendo do *honeypot*. Nestes casos simplesmente ignoramos o erro de mapeamento e consideramos que os dados trafegam de AS_1 para AS_2. Esta heurística impacta a completude dos nossos resultados (quando ignoramos um AS), mas *não* impacta a correção dos resultados (pois os dados trafegaram entre os ASes considerados, mesmo que indiretamente). Obtemos a tabela de roteamento BGP do AS que hospeda um dos *honeypots* e verificamos que 89% das rotas convertidas de endereços IP para ASes são idênticas às rotas BGP (98% tem diferença de até um AS).

[3]http://www.team-cymru.org/Services/ip-to-asn.html

Utilizamos a base de dados de relações (políticas de roteamento) entre ASes disponibilizada pela CAIDA [Luckie et al. 2013]. Neste artigo assumimos que ASes clientes pagam a ASes provedores para obter conectividade com o resto da Internet e que ASes parceiros (peer) trocam tráfego sem custo para ambas as partes. Estas suposições são alinhadas com suposições em outros trabalhos na literatura [Gao 2001, Luckie et al. 2013, Oliveira et al. 2010].

3. Avaliação do custo do tráfego de *spam*

Nesta seção, apresentamos os resultados obtidos através da metodologia apresentada na seção 2. Para não comprometer a identidade dos *honeypots* omitimos suas localizações exatas e anonimizamos as redes hospedeiras.[4] Primeiramente apresentamos um estudo de caso de um *honeypot* no Brasil, o BR-02 (seção 3.1). Este estudo de caso, além de ilustrar como a análise de resultados foi feita, revela importantes conclusões práticas sobre como filtros bem colocados na rede podem bloquear grande parte do *spam* mais próximo à origem. Por fim generalizamos os resultados encontrados para BR-02 para os outros cinco *honeypots*, mostrando que os resultados encontrados são aplicáveis ao tráfego *spam* de forma geral e identificando quais são as redes mais oneradas pelo tráfego de *spam* (seção 3.2).

3.1. Estudo de caso do *honeypot* BR-02

As rotas dos mapas das figuras 2 e 3 sintetizam os ASes mais utilizados nas rotas obtidas pelos traceroutes coletados através de uma máquina do PlanetLab no AS do *honeypot* BR-02. O mapa da figura 2 mostra os ASes que mais apareceram nas rotas entre a máquina do PlanetLab e as máquinas que enviaram *spam*. A direção das arestas mostra o sentido do *traceroute* e o tipo da linha a relação comercial. As variáveis sobre as arestas mostram a porcentagem do volume de mensagens de *spam* indo em direção ao *honeypot* que passa pela aresta.

O mapa da figura 2 contém alguns pontos interessantes. O primeiro é a aresta entre o AS do *honeypot* BR-02 e um de seus provedores, a Level 3 (AS3356), onde cerca de 77% do volume do tráfego, é trafegado. Além disso, existe um grande número de endereços IP de origem (24107) cujas mensagens chegam ao *honeypot* pela Level 3. Neste caso, conforme será detalhado na seção 3.2, é o enlace que mais gera custos para o AS do *honeypot* BR-02. O segundo ponto de interesse é a aresta entre o *honeypot* BR-02 e a Hurricane Electric (AS6939), onde 20% do volume total é trafegado. Neste enlace, tem-se um baixo número de endereços IP de origem que enviam um grande número de mensagens (28,4% do total). Realizando uma análise mais profunda, verificamos que 75 dos 82 endereços IP utilizam o protocolo SOCKS, indicando que esse enlace é muito usado por tráfego de *spam* gerado por servidores dedicados.

Finalmente, o terceiro ponto de interesse é entre a HiNetUSA (de Taiwan, AS9680) e a HiNet (AS3462), que enviam cerca de 51% do volume trafegado. Essa rota é interessante visto que a HiNetUSA recebe o *spam* da HiNet e pode estar dividindo esse tráfego em várias rotas, de forma a baratear despesas com tráfego de rede. Isso acontece pelo fato que, em grande parte dos contratos entre ASes, o custo pela

[4] Como nosso objetivo é continuar monitorando a rede de forma a estudar e detectar mudanças no comportamento dos *spammers*, precisamos proteger a identidade dos *honeypots* para preservar sua utilidade.

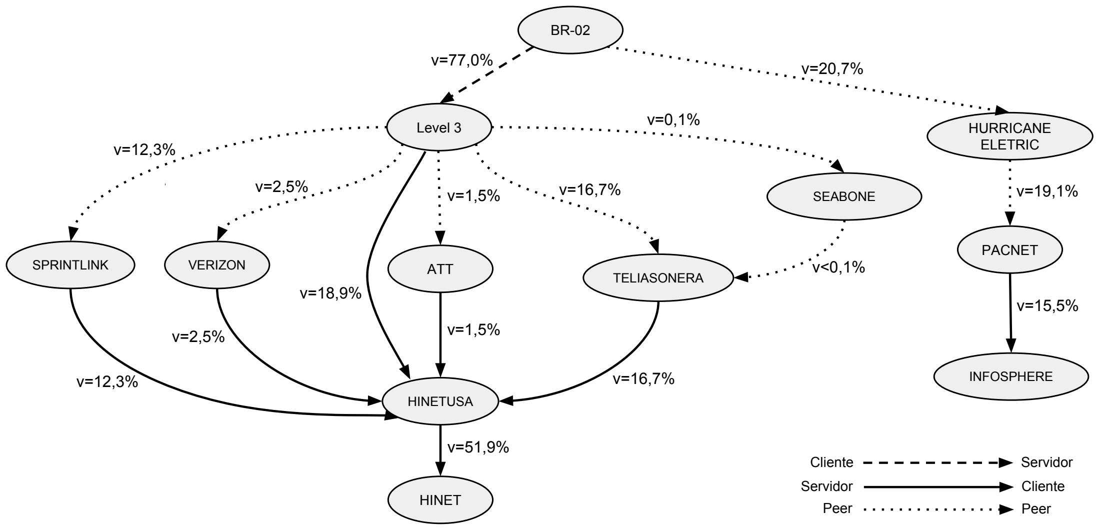

Figura 2. Mapa dos ASes mais utilizados entre o *honeypot* e as máquinas que enviam *spam*.

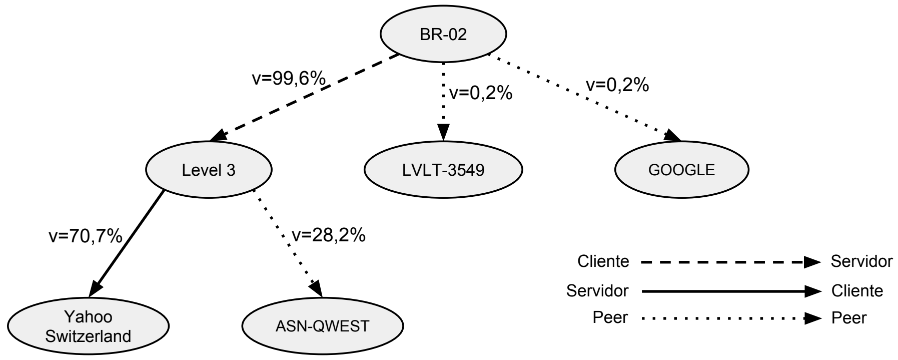

Figura 3. Mapa dos ASes mais utilizados entre o *honeypot* e os domínios de destino.

banda é proporcional ao 95º percentil da banda consumida em intervalos de cinco minutos [Dimitropoulos et al. 2009, Valancius et al. 2011]. Em uma análise minuciosa, verificamos que os prefixos anunciados pela HiNetUSA para seus provedores[5] são disjuntos, o que distribui e reduz o 95º percentil do tráfego. Entretanto, não pode-se afirmar que a HiNetUSA está hospedando *spammers* visto que aproximadamente 98% dos endereços IP que utilizam essa rota usam o protocolo SMTP que, conforme explicado na seção 2.1, geralmente fazem parte de *botnets*.

O mapa da figura 3 é similar ao mapa da figura 2, mas mostra o mapa dos 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 na próxima seção, 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.[6] Em outras palavras, o volume de tráfego que circula entre os ASes mostrados na figura 3 é maior que o tráfego que circula entre os ASes mostrados na fi-

[5]Sprint (AS1239), Verizon (AS701), Telia (AS1299), AT&T (AS7018) e Level 3 (AS3356).

Tabela 3. ASes que mais pagam/recebem no BR-02 do *spammer* ao *honeypot*

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* BR-02, BR	66,5	Level 3, US (3356)	97,0
HiNetUSA, TW (9680)	44,1	HiNetUSA, TW (9680)	44,1
HiNet, TW (3462)	44,1	PacNet, HK (10026)	16,2
InfoSphere NTT PC, JP (2514)	14,0	TeliaSonera, SE (1299)	14,2
Internet INT Japan, JP (2497)	11,9	SprintLink (1239)	10,4

gura 2. 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 821. O tráfego poderia ser ainda maior caso a recomendação do RFC não fosse seguida.

De acordo com o mapa da figura 3, temos que o *honeypot* BR-02 transmitiria 99% do volume de *spam* de volta pela Level 3. Esse volume, 28 vezes maior que o volume que chega ao *honeypot*, aumenta ainda mais os custos de comunicação. Além disso, grande parte deste volume (70%) é repassado para o Yahoo, um dos maiores operadores de e-mail, possivelmente gerando grandes custos para esta rede. Portanto, um possível uso de filtros de *spam* no AS que hospeda o *honeypot* BR-02 evitaria replicação de mensagens e reduziria custos de rede não só no seu próprio AS mas também para o Yahoo. Note que após o *honeypot* encaminhar as mensagens de *spam*, o Yahoo não pode filtrá-las antes de recebê-las.

3.1.1. Análise de custos do BR-02

As rotas dos mapas 2 e 3 incitam um questionamento pertinente sobre quem paga e quem recebe pelo tráfego de *spam* gerado. As tabelas 3 e 4 mostram os principais ASes que são onerados e os principais ASes que lucram em relação ao volume enviado. Para realizar essa análise, consideramos as relações comerciais entre os ASes dessas rotas. Para relações cliente-provedor, contabilizamos custos para o cliente e lucro para o provedor proporcionais à quantidade de tráfego. Note que um provedor pode receber por volume de tráfego maior do que o volume recebido pelo *honeypot* caso ele receba o tráfego de um cliente e repasse a outro cliente. Para relações de parceria e relações não inferidas, nenhum tipo de contagem é realizado. Neste caso, o *honeypot* pode pagar por menos tráfego do que recebido se parte do tráfego chegar por um AS parceiro. Medimos o volume de tráfego por que 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 desta ser uma limitação do nosso trabalho, esta informação é sensível e provavelmente protegida por acordo de sigilo (NDAs) entre as partes.

Realizando uma análise do tráfego que sai do *spammer* em direção ao *honeypot* BR-02, a tabela 3 mostra os cinco ASes que mais pagaram e os que mais lucraram com este tráfego. Como esperado, o AS que mais perdeu, em tráfego, foi o AS do *honeypot*

[6] Por exemplo, um e-mail destinado a elverton@dcc.ufmg.br, dorgival@dcc.ufmg.br e jessen@cert.br precisa ser enviado aos servidores de e-mail do DCC/UFMG e do CERT.br.

Tabela 4. ASes que mais pagam/recebem no BR-02 do *honeypot* ao servidor de destino

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* BR-02, BR	1.898,7	Level 3, US (3356)	3.247,3
Yahoo-Switzerland, CH (42173)	1.346,4	Qwest, US (209)	538,1
KDDi Corp, JP (2516)	538,4	NTT-Comm, US (2914)	4,0
OCN NTT, JP (4713)	4,2	LVLT-3549, US (3549)	2,8
Microsoft Corp, US (8075)	2,7	TiNet-Backbone, DE (3257)	1,4

BR-02 seguido pela HiNetUSA. Entre os ASes que mais receberam, temos a Level 3 como maior beneficiária seguido da HiNetUSA. Neste caso, a HiNetUSA, que divide o tráfego entre seus provedores conforme analisado na seção anterior, está entre os que mais ganharam recebendo 44,1 GB de seus clientes e os que mais perderam enviando a mesma quantidade para seus provedores, ficando com saldo nulo. Entretanto, na prática, este resultado indica que a HiNetUSA obteve lucro, visto que o valor que um AS cobra para seus clientes é maior que o valor que ele paga para seus provedores. Dessa forma, o balanceamento de rotas realizado neste AS pode estar sendo feito para tentar tornar os custos menores.

Fazendo um estudo sobre o volume do tráfego que sairia do *honeypot* BR-02 em direção aos servidores de email, a tabela 4 mostra os ASes que mais perderam e os que mais ganharam com o tráfego. Conforme mencionado na seção anterior, as mensagens que chegam ao servidor SMTP têm uma cópia enviada para cada domínio distinto nos destinatários das mensagens. Isso representa uma amplificação no tráfego, conforme pode ser visto comparando o volume de tráfego entre as tabelas 3 e 4, onde o AS do *honeypot* BR-02 que antes pagava por um volume de 66,5 GB, passa a pagar por mais de 1.8 TB, representando um aumento de, aproximadamente, 2800%. Além disso, redes com servidores de destino como o Yahoo (AS42173), passam a ser oneradas por um volume significativo de tráfego. Essa amplificação afeta também os que mais recebem, como é o caso da Level 3, com um saldo positivo para mais de 3 TB recebidos. A Qwest (AS209) é outro AS que também lucraria caso as mensagens de *spam* do *honeypot* BR-02 fossem entregues aos destinos.

Este estudo de caso mostra a importância do esforço no combate ao *spam* na origem. Em particular, grandes provedores como Level 3, Qwest e Telia não têm incentivos para implantar filtros contra tráfego de *spam*. Mesmo sem cooperação de grandes provedores, redes de borda podem cooperar para filtrar o tráfego de *spam*. Em particular, se filtros fossem posicionados na HiNet, por exemplo, reduziriam o tráfego que chega ao *honeypot* em quase 52%. De forma similar, outro filtro na InfoSphere (AS2514) reduziria o tráfego de *spam* em mais 15%. Como consequência, esse volume de *spam* não chegaria a servidores de e-mail (como o *honeypot*) e não seria replicado para reenvio aos servidores de destino, reduzindo drasticamente o tráfego enviado aos destinatários e evitando desperdício de recursos. Por último, notamos que mesmo sem cooperação das redes que enviam grande quantidade de *spam* (como HiNet e InfoSphere), ainda seria possível filtrar aproximadamente 37% do tráfego em direção ao *honeypot* e parte do tráfego replicado para reenviar as mensagens até os destinatários.

Tabela 5. 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)
	AS *Honeypot* BR-01	90,5	Embratel,BR (4230)	90,6
	Embratel, BR (4230)	48,0	Verizon, US (701)	39,7
BR-01	HiNetUSA, TW (9680)	24,0	HiNetUSA, TW (9680)	24,0
	HiNet, TW (3462)	24,0	SprintLink, US (1239)	17,5
	ROSTelecom, RU (12389)	10,2	TiNet-Backbone, DE (3257)	11,9
	AS *Honeypot* NL-01	86,7	TiNet-Backbone, DE (3257)	69,9
	HiNet, TW (3462)	30,4	HiNetUSA, TW (9680)	30,4
NL-01	HiNetUSA, TW (9680)	30,3	KPN Eurorings, NL (286)	20,7
	InfoSphere, JP (2514)	22,8	PacNet, HK (10026)	20,4
	OCN NTT, JP (4713)	5,6	TeliaNet, SE (1299)	16,3
	AS *Honeypot* US-03	58,4	XO Comm, US (2828)	32,1
	HiNet, TW (3462)	22,5	TWCable-Backbone, US (7843)	26,3
US-03	HiNetUSA, TW (9680)	19,7	Level 3, US (3356)	25,7
	CW CABLE AND WIRELESS WW, GB (1273)	5,4	HiNetUSA, TW (9680)	22,5
	TWCable-Backbone, US (7843)	5,3	TeliaNet, SE (1299)	13,7
	AS *Honeypot* UY-01	77,2	SprintLink, US (1239)	111,2
	HiNetUSA, TW (9680)	23,0	HiNetUSA, TW (9680)	23,0
UY-01	HiNet, TW (3462)	23,0	NTT-Comm, US (2914)	15,0
	InfoSphere, JP (2514)	12,3	TWGATE-AP, TW (9505)	9,4
	TWGATE-AP, TW (9505)	9,4	ROSTelecom, RU (12389)	9,0

3.2. 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 e UY-01). A tabela 5 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 pode-se notar, em todos os casos, os ASes dos *honeypots* são os que mais são onerados indicando que, na prática, ASes que recebem *spam* são os mais prejudicados. De forma similar, também vemos que os ASes que enviam a maior quantidade de *spam*, como a HiNet, também é onerada.

Um outro fato interessante é a presença da HiNetUSA em todos os quatro *honeypots* da tabela 5, dentre os mais onerados e também dentre os que mais recebem. Como observado para o *honeypot* BR-02, grande parte dos *spammers* que utilizam rotas através da HiNetUSA usam o protocolo SMTP, em todos os *honeypots* (não mostrado). Isto reforça o fato que o *spam* enviado através da HiNetUSA é oriundo de *botnets* e não podemos afirmar que este AS está sendo conivente. Porém podemos afirmar que filtros de *spam* instalados na HiNet reduziriam o tráfego de *spam* de forma global.

A tabela 6 mostra o mesmo dado que a tabela 5 para as rotas trafegadas pelas mensagens enviadas do *honeypot* ao servidor de destino. A relação entre o tráfego pago pelo *honeypot* na tabela 5, e o tráfego pago pelo *honeypot* na 6 segue um padrão bastante pertinente. Como pode-se observar, o volume pago pelos *honeypots* é muito menor na tabela 5 do que na tabela 6. Isso se deve ao fato discutido sobre a amplificação do tráfego que as mensagens de *spam* podem ocasionar ao atingir um servidor SMTP. Neste caso, o volume pago pelo *honeypot* na saída pode aumentar mais de 3000%, como no caso do *honeypot* NL-01. Em posse dessa visão mais global, é possível mostrar como o uso de filtros de *spam* que impeçam mensagens de atingir um servidor SMTP podem reduzir o

Tabela 6. 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* BR-01	2.230,9	Embratel, BR (4230)	2.230,9
	MailRu, RU (47764)	475,0	RETN Limited, UA (9002)	475,0
BR-01	Embratel, BR (4230)	61,4	Verizon, US (701)	104,9
	HiNetUSA, TW (9680)	47,3	HiNetUSA, US (9680)	47,3
	HiNet, TW (3462)	47,3	BTN, US (3491)	8,8
	AS *Honeypot* NL-01	3.866,8	POPPE, US (4525)	177,8
	Yahoo-JP-AS-AP, JP (24572)	177,8	GigaInfra, JP (17676)	177,8
NL-01	GigaInfra, JP (17676)	177,8	ROSTelecom, RU (12389)	156,2
	RTComm, RU (8342)	166,1	Verizon, US (702)	14,5
	Sovam, RU (3216)	14,5	IpTransit, US (46786)	12,6
	AS *Honeypot* US-03	146,0	XO-AS15, US (2828)	136,1
	TransTelecom, RU (20485)	56,4	Level 3, US (3356)	125,6
US-03	HiNet, TW (3462)	49,5	HiNetUSA, TW (9680)	49,5
	HiNetUSA, TW (9680)	49,5	Verizon, US (701)	48,9
	MailRu, RU (47764)	47,5	TransTelecom, RU (20485)	47,5
	AS *Honeypot* UY-01	1.478,2	SprintLink, US (1239)	1.486,5
	SeedNet, TW (4780)	9,0	Level 3, US (3356)	9,3
UY-01	BTN-ASN, US (3491)	8,5	BTN-ASN, US (3491)	8,5
	HiNet, TW (3462)	3,4	HiNetUSA, TW (9680)	3,3
	HiNetUSA, TW (9680)	3,3	ChinaNet, CN (4134)	2,6

tráfego da rede. O impacto é bem maior que os filtros utilizados nos servidores de destino que não impedem todo este gasto de recursos.

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*, a quantidade que eles recebem é sempre maior. A Embratel é um ótimo estudo de caso neste cenário, visto que ela apresenta este comportamento tanto nas rotas entre o *spammer* e o *honeypot* quanto nas rotas entre o *honeypot* e os servidores de destino. Por exemplo, no *honeypot* BR-01, ela aparece na tabela 5 pagando por 48,0 GB de tráfego, mas recebe por 90,6 GB. De forma similar, a Embratel paga por 61,4 GB de tráfego enviado do *honeypot* aos destinatários (tabela 6), mas recebe por 2.230,9 GB de tráfego. A Embratel consegue reduzir custos e obter lucro trafegando mensagens de *spam* graças a uma parceria de troca de tráfego com a Hurricane Electric. A TW Cable apresenta um comportamento semelhante, mas em uma proporção menor, recebendo quatro vezes mais do que paga, como pode ser observado na tabela 5.

4. Trabalhos Relacionados

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. 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 daquele prefixo. Para maximizar a cobertura do espaço de endereçamento IP, estas bases utilizam anúncios de rotas coletados por diversos roteadores BGP conectados à Internet (como os roteadores dos projetos RouteViews e RIPE RIS) bem como informações de alocação de prefixos de registros como ARIN, RIPE e LAC-

NIC. [Chen et al. 2009] propuseram diversas heurísticas para correção de erros comuns inseridos pelo mapeamento de endereços IPs em ASes. Em particular, eles observaram que endereços IPs pertencentes a pontos de troca de tráfego (PTT) podem aparecer entre dois ASes membros do PTT e que ASes podem usar endereços IPs "emprestados" de outros ASes; ambos casos levam à criação de parcerias falsas. Em nosso trabalho implementamos e utilizamos apenas algumas das heurísticas propostas por [Chen et al. 2009].

Os primeiros algoritmos para identificação de relações entre ASes foram propostos por [Gao 2001]; 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].

Caracterização de Tráfego de Spam na Internet. Existem vários trabalhos sobre caracterização de tráfego na Internet.[7] Mais relacionados a este artigo são trabalhos sobre a caracterização de propriedades do tráfego de *spam*. Por exemplo, [Ramachandran and Feamster 2006] mostram que diversos elementos do tráfego de spam podem ser usados para tentar identificar sua transmissão através da rede. Mais importante do ponto de vista deste estudo são trabalhos que usam dados de rotas para identificar ASes maliciosos [Konte and Feamster 2011, Ramachandran and Feamster 2006]. De forma similar, neste trabalho identificamos práticas de engenharia de tráfego suspeitas.

Custos de Spam e Tráfego na Internet. Sobre a questão de custo do spam, [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 artigo. 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]. Estes 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 mostramos que redes de borda são as mais oneradas pelo tráfego de *spam* e discutimos como ASes aparentam tentar minimizar o custo para enviar o tráfego de *spam* e como redes de borda são prejudicadas.

Também relacionados às nossas análises são propostas para filtrar mensagens de e-mail na origem e reduzir o custo de propagação de *spam* pela Internet [Las-Casas et al. 2013]. Nossa metodologia permite identificar quais redes têm incentivos para implantar tais filtros, facilitando a cooperação e implantação destas técnicas.

5. Conclusão e Trabalhos Futuros

Neste trabalho, objetivamos lançar mais luz sobre os custos gerados pela prática de *spamming* através de mensagens capturadas por cinco *honeypots* em redes distintas. Realiza-

[7]Por exemplo, o relatório *Global Internet Phenomena* da Sandvine apresenta e discute tendências de tráfego na Internet a cada seis meses (https://www.sandvine.com/trends/global-internet-phenomena/).

mos medições com *traceroutes* a partir das plataformas RIPE Atlas e PlanetLab que, combinadas com técnicas para mapeamento de endereços IP em sistemas autônomos (AS), permitiram inferir as rotas utilizadas pelos *spammers*. Além disso, utilizamos resultados recentes sobre inferências de relações comerciais entre ASes para quantificar os custos gerados pelo tráfego de *spam* em cada rede.

Nossos resultados mostram que algumas redes são sistematicamente oneradas pelo tráfego de *spam* mas que podem cooperar para reduzir bastante o tráfego filtrando mensagens de *spam* na origem. Além disso, mostramos que ASes que enviam grande quantidade de *spam* aparentam utilizar práticas de engenharia de tráfego para reduzir custo. Por fim, quantificamos o efeito amplificador que as mensagens de *spam* têm ao alcançar servidores SMTP e a redução drástica deste tráfego de *spam* caso fossem instalados filtros para impedir que essas mensagens atinjam tais servidores.

Como trabalho futuro pretendemos realizar essas análises para diferentes períodos, de forma a entender a dinâmica dos custos do tráfego de *spam*, por exemplo, em função de mudanças de roteamento. Além disso, com monitoramento constante podemos identificar quais ASes estão tendo os seus custos aumentados e alertá-los, servindo como incentivo para que os mesmos utilizem filtros para reduzir o volume de *spam* trafegado.

Agradecimentos

Este trabalho foi parcialmente financiado por NIC.BR, Fapemig, CAPES, CNPq e InWeb. Gostaríamos de agradecer, também, ao Matt Calder, da Universidade do Sul da Califórnia (EUA), pelo scripts fornecidos para a utilização da plataforma RIPE Atlas.

Referências

Anderson, D. S., Fleizach, C., Savage, S., and Voelker, G. M. (2007). Spamscatter: Characterizing Internet Scam Hosting Infrastructure. In *USENIX Security Symposium*.

Chen, K., Choffnes, D. R., Potharaju, R., Chen, Y., Bustamante, F. E., Pei, D., and Zhao, Y. (2009). Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes from P2P Users. In *Proc. ACM CoNEXT*.

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

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., and kc claffy (2014). Inferring Complex AS Relationships. In *Proc. IMC*.

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

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

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

Luckie, M., Huffaker, B., Claffy, K., Dhamdhere, A., and Giotsas, V. (2013). AS Relationships, Customer Cones, and Validation. In *Proc. IMC*.

Madhyastha, H., Isdal, T., Piatek, M., Dixon, C., Anderson, T., Krishnamurthy, A., and Venkataramani, A. (2006). iPlane: an Information Plane for Distributed Services. In *Proc. USENIX OSDI*.

Mühlbauer, W., Uhlig, S., Fu, B., Meulle, M., and Maennel, O. (2007). In Search for an Appropriate Granularity to Model Routing Policies. In *Proc. ACM SIGCOMM*.

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

Oliveira, R., Pei, D., Willinger, W., Zhang, B., and Zhang, L. (2010). Quantifying the Completeness of the Observed Internet AS-level Structure. *IEEE/ACM Trans. Netw.*, 18(1):109–122.

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

Ramachandran, A. and Feamster, N. (2006). Understanding the Network-level Behavior of Spammers. In *Proc. ACM SIGCOMM*.

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

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

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

Symantec (2014). Internet Security Threat Report, Volume 19. Online.

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