PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Programa de Pós-Graduação em Informática

CARACTERIZAÇÃO E ANÁLISE DO COMPORTAMENTO DE DESTINATÁRIOS E REMETENTES DE SPAMs

Thaína Amélia de Oliveira Alves

Belo Horizonte

2011

Thaína Amélia de Oliveira Alves

CARACTERIZAÇÃO E ANÁLISE DO COMPORTAMENTO DE DESTINATÁRIOS E REMETENTES DE SPAMs

Dissertação apresentada ao Programa de Pós-Graduação em Informática como requisito obrigatório para qualificação ao Grau de Mestre em Informática pela Pontifícia Universidade Católica de Minas Gerais.

Orientador: Humberto T. Marques Neto

Belo Horizonte

2011

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

A474c

Alves, Thaína Amélia de Oliveira
Caracterização e análise do comportamento de destinatários e remetentes de Spams / Thaína Amélia de Oliveira Alves. Belo Horizonte, 2011.
60f.: il.

Orientador: Humberto Torres Marques Neto
Dissertação (Mestrado) – Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Informática.

1. Spam (Mensagens eletrônicas). 2. Correio eletrônico. 3. Cliente/servidor (Computação). I. Marques Neto, Humberto Torres. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Informática. III. Título.

CDU: 681.3.01

Thaína Amélia de Oliveira Alves

CARACTERIZAÇÃO E ANÁLISE DO COMPORTAMENTO DE DESTINATÁRIOS E REMETENTES DE SPAMs

Dissertação apresentada ao Programa de Pós-Graduação em Informática como requisito parcial para qualificação ao Grau de Mestre em Informática pela Pontifícia Universidade Católica de Minas Gerais.

Humberto Torres Marques Neto –
PUC Minas

Virgílio Augusto Fernandes de Almeida –
UFMG

Artur Ziviani – LNCC/MCTI

Luis Enrique Zárate Gálvez – PUC Minas

Belo Horizonte, 16 de Dezembro de 2011.

Aos meus pais, Aparecida e Paulo, pelo incentivo, pela paciência e por me proporcionar mais essa importante conquista.

AGRADECIMENTOS

Agradeço em primeiro lugar aos meus pais, Paulo e Aparecida, pelo compreensão e incentivo durante toda a vida e por darem condições plenas para que eu alcançasse esta conquista. Não existe palavras que expressem o meu amor e gratidão a vocês. À meu irmão, Rafael, pelo seus conselhos e palavras de motivação para seguir em frente quando o desespero tomava conta. Àо Pedro, pelo carinho e total compreensão nos dias em que estive ausente me dedicando ao Mestrado. À madrinha Dedé e à vovó Terezinha pelas constantes orações e torcida pelo meu sucesso.

Agradeço ao meu orientador, Humberto T. M. Neto, pela excelente orientação ao longo desta pesquisa, contribuindo sempre com idéias, questionamentos e críticas, além de sempre estar presente em qualquer momento que precisei, compreendendo meus horários limitados devido ao trabalho. Minha gratidão pela confiança depositada e por ser um dos responsáveis por essa conquista.

Às minhas amigas da PUC e aos meus amigos do CPE, que várias vezes me proporcionaram momentos de descontração tão necessários e precisaram escutar desabafos e relatos do meu trabalho. À FITec e aos colegas de trabalho, pelo apoio, pela compreensão e por compartilharem no dia-a-dia momentos importantes da trajetória percorrida até aqui, em especial ao Daniel Paranhos que acompanhou mais que relatos, mas também angústias e alegrias e sempre me motivou a cumprir esta jornada.

Aos professores e funcionários do Programa de Mestrado em Informática da PUC-MG com os quais foi possível amadurecer e aprofundar meus conhecimentos em ciência da computação. À equipe técnica do provedor de e-mails por disponibilizar os dados base para esta pesquisa e contribuir com informações solicitadas durante a pesquisa. Agradeço também aos colegas de Mestrado da UFMG e ao Prof. Virgílio Almeida, pois através na disciplina de "Redes Complexas: Teoria e Algoritmos" pude enriquecer e aprofundar conhecimentos essenciais para o desenvolvimento dessa pesquisa.

Agradeço a todos que não apareceram na lista acima, mas, sabem que de longe ou perto contribuíram de alguma forma para a realização dessa pesquisa.

RESUMO

O utilização da Internet vem aumentando muito nos últimos anos. Neste contexto, percebe-se que o envio de spams se tornou um grande problema. O aumento das redes formadas por usuários de e-mails e do conteúdo malicioso existente nelas, motiva a identificação de possíveis efeitos negativos que podem ser causados ao provedor de correio eletrônico. Este trabalho utiliza métricas de redes complexas (popularidade e a conectividade), para apresentar a caracterização de remetentes e destinatários de spams e de e-mail legítimos que possuem contas de e-mail no provedor de mensagens eletrônicas em estudo, afim de analisar e identificar o comportamento destes usuários. Os registros dos remetentes e destinatários de spams estão presentes em um *dataset* com dados reais gerado pelo filtro de spam de um provedor de Internet corporativo. Já os remetentes e destinatários de e-mails legítimos estão presentes em um outro *dataset* com dados reais gerado do mesmo provedor de e-mails utilizado para coletar os usuários de spams. Os resultados mostram que a utilização das métricas de redes complexas (popularidade e conectividade) auxiliam a identificação de usuários maliciosos (spammers e destinatários). Através da análise da popularidade dos destinatários de mensagens eletrônicas em ambas os *datasets* (spams e e-mails legítimos), observou-se que poucos usuários destinatários possuem alta popularidade nas redes, ou seja, existe um concentração de envio de spams e também e-mails legítimos para um conjunto restrito de usuários finais do provedor. Este conjunto de usuários destinatários foi analisado com o propósito de entender algumas de suas características que podem, de alguma forma, atrair um volume maior de mensagens indesejadas que, provavelmente, serão processadas e descartadas no seu destino. Identificar o comportamento dos usuários destinatários "foco" de spam é uma tarefa que pode contribuir para o desenvolvimento e evolução de técnicas para o gerenciamento de contas de usuários de um provedor, possibilitando assim estabelecer uma melhoria nos serviços de e-mails.

Palavras-chave: spams, servidores de e-mail, mensagens eletrônicas.

ABSTRACT

The communication using Internet resources is proving to be a very important task carried out almost daily by people. Specifically, the email exchange among these people is one of the most common communication activities which take a great deal of senders an recipients time-of-work. Moreover, the increase of email misuse/abuse has resulted in an increasing volume of spams over recent years, requiring a well-done management of the email services infrastructure. This research uses two metrics (popularity and connectivity) for characterizing senders and recipients of spam and e-mails that have e-mail accounts on the provider of electronic messages, in order to identify and analyze the behavior of users. The records of the senders and recipients of spam are present in a dataset generated by the real spam filter from an e-mail provider (spam network). The sender and recipients of legitimate emails are recorded on the different dataset generated by the provider mentioned (email network). The results show that the analysis of these metrics can improve the effectiveness of the identification of email addresses used by spammers and also the email accounts which receive a large number of unwanted and/or malicious messages. Analyzing the popularity of the recipients in both datasets (spams and legitimate emails), we observed that there was a concentration of spamming and e-mails for a small group of users. This group was analyzed in order to understand their characteristics that, in some way, attracting larger quantities of spam that are processed and discarded on their destination. Identifying the spammed users' behavior is a task that can contribute to the development and evolution of techniques for managing user accounts of providers, thus enabling an improvement in services provide e-mails.

Keywords: spams, emails server, eletronic messages.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O desenvolvimento e a popularização da Internet vem crescendo muito nos últimos anos. Neste contexto, percebe-se que os e-mails maliciosos e/ou não-solicitados enviados em massa (spam)[1] se tornaram um grande problema de abuso da infraestrutura de redes da atualidade. Relatórios recentes mostram que o Brasil está presente entre os três países que mais disseminam spams na Internet, juntamente com o Estados Unidos e a Índia (CISCO, 2011). O relatório do Labs (2011) mostra que em Julho de 2011 a taxa de spams por e-mail trafegado aumentou 4,9% comparado ao mês anterior, ou seja 1 em cada 1.29 mensagens de e-mail é spam.

Em busca de conter esse problema, surgiram vários mecanismos de combate a mensagens maliciosas e/ou não desejadas enviadas em massa, tais como, filtros *antispam*, lista de spammers, entre outros. Apesar da existência desses mecanismos dedicados ao bloqueio de spam, ainda nota-se a chegada de muitas mensagens indesejadas na caixa de entrada dos destinatários. Ou seja, ainda há grandes esforços dedicados ao bloqueio de spams, pois as mensagens não desejadas têm representado cerca de 80% de todos e-mails trafegados na Internet (SYMANTEC, 2011).

A melhoria dos mecanismos *antispam* pode trazer muitos benefícios para os usuários finais que deixariam de ter suas caixas de entrada repletas de e-mails não desejados. Entretanto, a filtragem realizada por esses mecanismos pode ser ineficiente devido a falta de conhecimento do comportamento dinâmico de spammers[2] e também do comportamento dos próprios destinatários de spams. O relatório da Nucleus-Research (2007), evidencia que o spam não filtrado, ou seja, que precisa ser tratado pelo próprio usuário, acarreta uma queda de produtividade em cerca de 1,2% por empregado ao ano, causando assim prejuízos para as empresas.

Além disso, essa grande quantidade de spams que circulam na Internet pode afetar também o desempenho dos provedores de e-mail e, ainda, causar desperdício de recursos para o tratamento do tráfego de spam na rede (TWINING *et al.*, 2004). Prejuízos dessa natureza podem ser minimizados com a melhoria dos mecanimos *antispam* e também

[1] Definição de SPAM baseada na definição da *Spamhaus* (http://www.spamhaus.org/)
[2] Autores de mensagens maliciosas e/ou não desejadas enviadas em massa (spam).

com um melhor gerenciamento das contas de e-mails por parte dos provedores. Ou seja, é importante analisar as redes de e-mails em duas abordagens: a partir da análise do comportamento dos spammers, e a partir da análise do comportamento dos destinatários de spams. Essa última abordagem é o foco deste trabalho, o qual apresenta análises até o nível do usuário final.

O aumento das redes formadas por usuários de e-mails e do conteúdo malicioso existente nelas, motiva a identificação de possíveis efeitos negativos que podem ser causados ao provedor de correio eletrônico. A interação entre os usuários de mensagens eletrônicas tem estrutura semelhante a uma rede complexa, a qual é definida em (EASLEY; JON, 2010) como uma rede que possui uma topologia com características específicas, tais como, alto coeficiente de agrupamento e reciprocidade.

Neste trabalho a análise da popularidade e da conectividade (métricas de redes complexas) foram utilizados com o propósito de se compreender algumas dimensões do comportamento dos usuários de e-mail. De acordo com (EASLEY; JON, 2010), a popularidade é um fenômeno caracterizado por desequilíbrios extremos. No contexto deste trabalho, espera-se que poucos destinatários que recebem muitos spams, tenham um comportamento, relacionado ao envio/recepção de e-mails, diferente da maioria dos destinatários que recebem uma menor quantidade de spams. Já a conectividade avalia se os remetentes ao enviarem spams atingem os destinatários de forma regular, possuindo conexão com vários destinatários.

Diversos trabalhos na área de tráfego malicioso, buscam caracterizar o comportamento dos remetentes de spam (spammers) e identificar características desses que se diferem dos usuários legítimos de e-mail. Neste trabalho além de analisar a popularidade e conectividade dos spammers busca-se, principalmente, entender o comportamento dos destinatários "foco" de spams.

Portanto, este trabalho caracteriza e analisa o comportamento de destinatários de spams e de e-mails legítimos de um provedor de correio eletrônico, buscando identificar possíveis usuários "foco" de recepção de spam. As análises são realizadas com base, principalmente, na popularidade dos remetentes e destinatários de mensagens eletrônicas, reconstituídas a partir de dois *datasets*. O primeiro conjunto de dados foi gerado por um filtro *antispam* de um provedor corporativo de e-mails (rede de spams) e o segundo contém informações dos e-mails legítimos dos usuários deste mesmo provedor (rede de e-mails).

Dessa forma, foi possível verificar a relação entre os usuários dessas duas cargas de trabalho e ainda classificá-los em dois grupos: *Corporativo* e *Pessoal*. Na visão do provedor, a constatação de usuários que recebem muito spams e e-mails e a identificação

do comportamento desses usuários pode auxiliar a detecção, por exemplo, de contas que se tornam inviáveis de serem gerenciadas e, em alguns casos, ficam desativadas. Desta forma, os resultados deste trabalho pode contribuir com um melhor gerenciamento das contas de usuários de correio eletrônico de um provedor de serviços, e ainda servir de referência para a implantação de políticas de tratamento de spams.

O restante deste trabalho está organizado em 5 capítulos. Os trabalhos relacionados são discutidos no Capítulo 2 que apresenta técnicas utilizadas para o combate ao spam, e também trabalhos sobre as características e comportamento de spammers, em contrapartida com características de usuários legítimos de e-mails, além de apresentar teorias que permitem modelar e analisar redes de usuários de troca de e-mails. No Capítulo 3 é descrita a metodologia de caracterização dos dados deste trabalho, onde apresenta o processo de análise do comportamento de usuários de e-mails maliciosos e legítimos quantificando e qualificando os registros presentes nos conjuntos de dados em estudo. O Capítulo 4 apresenta a análise dos resultados relevantes para este trabalho, como por exemplo, a popularidade dos usuários destinatários de spams e a relação desses com os usuários destinatários de e-mails legítimos. No Capítulo 5 é apresentada a conclusão deste trabalho e os possíveis trabalhos futuros.

2 TRABALHOS RELACIONADOS

A literatura apresenta uma série de trabalhos que buscam desenvolver e aprimorar técnicas contra spammers, além de pesquisas que buscam entender como os spammers se comportam e o quanto as mensagens maliciosas que circulam na Internet são prejudiciais tanto para os usuários finais quanto para provedores de serviço de correio eletrônico. Os trabalhos relacionados a este estudo foram divididos em subseções.

Na Subseção 2.1 são apresentadas as técnicas mais usuais e difundidas de combate ao spam, na Subseção 2.2 são apresentados estudos que caracterizam as cargas de trabalho de e-mails legítimos para então contrapor com a seção 2.3 onde são listados os trabalhos que buscam identificar o comportamento dos spammers. Na seção 2.4 são apresentados alguns conceitos da teoria de redes complexas, relevantes para a caracterização do comportamento de usuários remetentes e destinatários de spam e e-mails legítimos.

2.1 Técnicas Anti-spam

Devido ao fato do envio de spam (mensagens eletrônicas maliciosas e/ou não solicitadas enviadas em massa) ter se tornado um dos grandes problemas que atingem os usuários de e-mail da Internet, diversas técnicas foram criadas e desenvolvidas com a intenção de contê-los. Usualmente as técnicas buscam bloquear os spammers, não levando em conta o usuário final que pode também influenciar na melhoria do combate aos spams.

A técnica mais usual de combate ao spam é a utilização de filtros que impedem que os spams alcancem a caixa de entrada dos usuários. Para auxiliar esses filtros, também são utilizadas técnicas de classificação dos usuários quanto a sua confiabilidade, adicionando em *blacklists* aqueles que não são confiáveis e em *whitelists* os usuários considerados confiáveis. Esta seção apresenta as técnicas mais usuais de combate as mensagens não solicitadas.

O filtro anti-spam é a técnica mais difundida na tentativa de bloqueio do spam. Porém, existe uma grande dificuldade em afirmar a eficácia dos filtros quanto ao bloqueio de mensagens que são de fato não legítimas, pois, existe a questão de evitar os

falsos positivos. Os falsos positivos são mensagens que não são spams de fato, porém são classificadas como tal erroneamente, levando usuários a não receber mensagens legítimas.

Portanto, os trabalhos buscam aprimorar o funcionamento dos filtros *antispam* com intuito de diminuir a taxa de falsos positivos nas classificações sem diminuir os verdadeiros positivos. Tal fato, pode ser visto em Stolfo *et al.* (2006), onde foi implementado um *framework* que incorpora estratégias de vários algoritmos de aprendizagem de máquina em conjunto com mineração de dados para modelar o comportamento de usuários de e-mail individualmente. Para isso é necessário conhecer todo o conjunto de mensagens recebidas e enviadas por cada usuário. Esta ferramenta foi utilizada com sucesso para agrupar e classificar grupos de usuários de e-mail semelhantes e detectar possíveis usuários spammers, apresentando uma eficácia de 99% com uma taxa de 0.025% de falsos positivos. Pode ser visto que tal trabalho apresenta uma taxa baixa de falto positivo, tal fato pode representar uma forte contribuição nessa área de combate a spams.

Como apresentado acima, no trabalho de Stolfo *et al.* (2006) são analisados os comportamentos dos usuários de e-mails individualmente, porém existe também estudos que se baseiam no conteúdo das mensagens ao invés de ser no comportamento dos usuários. Sahami *et al.* (1998) apresentam uma abordagem de filtros muito popular que é a utilização da classificação baseada em *Naïve Bayesian*. *Bayesian filters* trabalham através da análise da palavras contidas dentro das mensagens e então calcula-se a probabilidade daquela mensagem ser spam. É válido ressaltar que esta probabilidade não é baseada apenas nas palavras que evidenciam que a mensagem é spam, mas também se baseia nas palavras que não são consideradas originárias de spammers. Para calcular essa probabilidade são utilizados algoritmos de aprendizagem de máquina para treinar os *Bayesian filters* utilizando de redes de palavras que estão presentes nos spams e redes de palavras presentes em e-mails legítimos. A vantagem desse filtro é que são auto adaptáveis, porém os spams mais atuais e complexos tentam utilizar menos palavras consideradas perigosas (free, money, etc) e mais palavras confiáveis (*hi*, oi, etc) para tentar enganar os filtros.

Seguindo a linha de raciocínio da técnica citada acima, o estudo de Goodman, Cormack e Heckerman (2007) também apresenta uma técnica para a filtragem de spam com base na comparação do conteúdo das mensagens. As mensagens recebidas são comparadas com uma lista de spam já conhecida anteriormente a fim de determinar se o novo e-mail é spam ou mensagem legítima. Evidentemente, a técnica não irá funcionar se houver qualquer alteração no corpo das mensagens de spam, além de ser ineficiente contra novos spams que ainda não fazem parte da lista previamente existente. Talvez ao utilizar tais técnicas em conjunto com a apresentada em Stolfo *et al.* (2006) seria possível

obter maior sucesso na comparação das mensagens recebidas ao agrupá-las aos usuários com comportamentos semelhantes.

Entre as técnicas que consideram o comportamento dos spammers como foco de análise, o estudo de Ramachandran, Feamster e Vempala (2007) apresenta um sistema chamado *SpamTracker*. O sistema utiliza uma técnica chamada bloqueio por comportamento que classifica os remetentes de e-mail (*hosts* de envio de e-mail) baseado em seu comportamento e não em sua identidade.O *SpamTracker* utiliza algoritmos de *clustering* eficientes que podem reagir rapidamente às mudanças de padrões de envio. Porém, a identidade e o comportamento de um *host* são determinados pelos domínios para onde o mesmo envia mensagens. Com o *SpamTracker* é possível agrupar tráfego de equipamentos de rede distintos numa mesma identidade, o que não seria interessante na filtragem.

Diferentemente dos trabalhos apresentados acima que se baseiam no conteúdo das mensagens e comportamento dos usuários, o trabalho de Castilho *et al.* (2010) se baseia em características do tráfego SMTP (*Simple Mail Transfer Protocol*), sob o ponto de vista do provedor de acesso, ou seja, busca-se diferenciar comportamentos legítimos de envio de e-mail de comportamentos suspeitos ou abusivos, analisando apenas dados obtidos da camada de rede de conexões SMTP. A carga de trabalho do provedor foi analisada utilizando algumas métricas, tais como, o número de transações SMTP realizadas por um usuário por unidade de tempo e o número de servidores de e-mail distintos contatados por ele. Em seguida foi utilizado um algoritmo de agrupamento para dividir os usuários segundo seus padrões de comportamento, quando foram identificados três perfis claramente distintos: usuários com uso baixo, médio e intenso de SMTP. Com tais informações, pode ser possível propor mecanismos que permitam o bloqueio de spams na origem.

Apresentando uma evolução do trabalho de Castilho *et al.* (2010) em Las-Casas *et al.* (2011) é proposto um método para detecção de spammers na rede de origem denominado *SpaDeS* (*Spammer Detection at the Source*), utilizando métricas que não requerem a inspeção do conteúdo das mensagens enviadas, utilizando uma técnica de classificação supervisionada (*Lazy Associative Classification* (LAC)), a qual foi aplicada em dois conjuntos de dados reais de um provedor de Internet de banda larga. Os método SpaDeS apresentou uma excelente efetividade, com taxa de acerto de 98% para usuários legítimos e 94% na classificação de spammers.

Cada vez mais os spammers têm buscado estratégias para que suas mensagens se assemelhem mais com mensagens legítimas, com propósito de enganar os filtros de spam. Com tais estratégias, os filtros precisarão ser cada vez melhores e mais treinados para distinguir entre mensagens maliciosas e legítimas. Para isso, deve-se unir técnicas

que identificam os comportamentos de spammers e não spammers afim de bloquear os usuários que agem de forma maliciosa. Além disso, a identificação de destinatários "foco" de spam como proposto neste trabalho pode representar um benefício no gerenciamento de contas de usuários para os provedores de serviço de correio eletrônico.

Outra técnica utilizada no combate as mensagens não solicitadas são as listas de e-mails que surgiram com o intuito de auxiliar o trabalho dos filtros de spam. Nos trabalhos de Weinstein (2003) e Cook *et al.* (2006) são apresentadas uma visão geral sobre a criação de listas, onde é proposta a utilização de *whitelists*, que listam os usuários ou *hosts* nos quais são considerados não spams. Assim, as mensagens de membros dessa lista são recebidas diretamente, sem haver a verificação do filtro, o que pode evitar os falsos positivos. Por outro lado, pode haver as listas de usuários considerados spammers, que serão membros de uma *blacklist* (COOK *et al.*, 2006). Porém essa técnica é facilmente contornada por e-mails forjados.

Para conter esses e-mails forjados, alguns trabalhos sugerem estratégias para identificar e caracterizar o emissor. Tal estratégia, pode ser vista em Ramachandran e Feamster (2006), onde é estudado como os spammers exploram a infraestrutura da rede para enviar suas mensagens, tentando determinar características de tráfego de rede como, por exemplo, faixas de endereços IP mais usadas para se enviar spam, tipo de abusos mais comuns e buscam identificar características de *botnets*[1](COOKE; JAHANIAN; MCPHERSON, 2005).

Em outro trabalho realizado por Li e Hsieh (2006), observou-se o surgimento de grandes grupos de IPs que enviam spams referenciando repetidas URLs contidas no conteúdo das mensagens de spam. Entre outras conclusões, os autores apresentam características da origem das mensagens e concluem que o envio de spams acontece em faixas restritas de endereços de IPs.

Existem também as *blackholes* que são listas de servidores considerados fontes de spam e dos quais as mensagens que originam desses não serão aceitas. O estudo de Serjantov e Clayton (2005) apresenta análises para a decisão de classificar um servidor como suspeito ou não, porém a questão nesse caso é decidir incluir um servidor suspeito na lista e perder as mensagens legítimas deste, ou não incluí-lo e continuar recebendo spams. Além disso, como avaliado em Paul *et al.* (2005), servidores existentes em diversas partes do mundo são contratados por spammers para o envio de mensagens maliciosas.

Apesar das estratégias citadas acima que buscam sempre dificultar o envio de e-mails por parte dos spammers, o combate da disseminação de spams através desses

[1] *Botnets são grupos de computadores infectados por malware, chamados de bots, controlados remotamente e utilizados muitas vezes para o envio de spam e para atacar outras redes de computadores. (COOKE; JAHANIAN; MCPHERSON, 2005)*

servidores não é simples, pois é necessário que todos servidores possuam a proteção. Não havendo essa adesão, os spammers apenas irão migrar de um servidor para outro, contornando a situação.

Lista de e-mails podem ser úteis no auxílio a filtros *antispam*, porém são facilmente contornadas e possuem forte impacto no falso positivo. Portanto, um melhor caminho seria conhecer o comportamento desses spammers a fim de definir estratégias para contê-los a partir de características mais estáveis.

2.2 Caracterização da Carga de trabalho de E-mails

Para obter um claro entendimento sobre cargas de trabalho de e-mails legítimos e maliciosos é necessário entender inicialmente como usuários legítimos se comportam para então identificar comportamentos não desejados. Existem diversos estudos que caracterizam e analisam diversos aspectos das cargas de trabalho de e-mail com propósito de delinear as características existentes no tráfego de e-mails legítimos.

Em Bertolotti e Calzarossa (2000) é realizada um extensa caracterização de várias cargas de trabalho de um servidor de e-mail, analisando características tais como, processo de chegadas das mensagens, tamanhos das mensagens, quantidade de destinatários por mensagem. Em continuidade a esse trabalho em Bertolotti e Calzarossa (2001) é proposto um modelo para o comportamento de usuários. Foi analisado o acesso de usuários aos servidores de e-mails (através do protocolo POP3), caracterizando tempo de acesso, número de mensagens por caixa de correio dos usuários, tamanho das caixas de correio. Os principais resultados mostram que o processo de chegada de e-mails pode ser representado por uma distribuição de Pareto, e que o tamanho dos e-mails é mais aproximado a uma distribuição Log Normal. Quanto a distribuição do número de recipientes por mensagem também possui cauda pesada, sendo que 94% dos e-mails são destinados para um único usuário destinatário.

O trabalho de Barabasi (2005) realiza uma caracterização de tráfego de e-mail em geral e aponta que, enquanto muitas ações humanas são aleatoriamente distribuídas ao longo do tempo, sendo bem aproximadas por processos de Poisson, o envio de e-mails é marcado pelo envio de rajadas de mensagens seguido de longos períodos de inatividade. Tal comportamento, é consequência de um processo de tomada de decisão baseado em prioridades o que leva o tempo de chegada dos eventos, no caso de mensagens, a ser melhor modelado por distribuições de cauda pesada, como a distribuição de Pareto. Este estudo encontra apoio em Bertolotti e Calzarossa (2000) onde também foi concluído que o processo de chegada das mensagens é melhor representado por distribuições de Pareto.

Tal fato, define e diferencia o comportamento dos usuários legítimos ao comparar com o comportamento de usuários maliciosos, como veremos na seção a seguir.

2.3 Caracterização da Carga de trabalho de Spam

Diversos trabalhos na área de caracterização de cargas de trabalho de e-mails separam a análise do tráfego malicioso e do tráfego legítimo. Ou seja, busca-se identificar separadamente as estratégias dos spammers e dos usuários legítimos tentando diferenciar comportamentos maliciosos de comportamentos legítimos.

Na busca por diferenciar tais comportamentos, o trabalho de Gomes *et al.* (2004) caracteriza uma carga de trabalho que possui e-mails recebidos e enviados por uma rede universitária, com base em critérios, tais como, tamanho das mensagens, processo de chegada e localidade temporal de endereços remetentes. Os resultados deste trabalho se assemelham aos encontrados em Bertolotti e Calzarossa (2001) quanto as características de e-mails legítimos.

Porém, Gomes *et al.* (2004) foram mais além ao caracterizar também os spammers, onde foi possível identificar que o comportamento malicioso (spam) e o comportamento legítimo se diferenciam em muitos dos aspectos. Por exemplo, existe uma diferença no tamanho médio das mensagens enviadas mostrando que e-mails maliciosos são geralmente de seis a oito vezes menores do que e-mails legítimos. Quanto ao número de e-mails no campo de destinatários (*to* e *cc*) e a localidade temporal foi visto que spammers enviam e-mails indiscriminadamente para seus destinatários alvos, não havendo relações sociais ou de localidade como apresentam as mensagens eletrônicas legítimas.

Estendendo a caracterização de spammers em Gomes *et al.* (2005) foi analisado também uma carga de trabalho de tráfego de e-mail, porém focando em características que não são facilmente alteradas relacionadas ao conteúdo das mensagens. Para isso, foram levantadas propriedades de grafos traçados entre remetentes e destinatários de mais de 330 mil e-mails recebidos e enviados por uma rede universitária, analisando características como grau de entrada e saída dos nós do grafo, o coeficiente de agrupamentos dos nós. Além dessas características, foi criada uma métrica chamada *Communication Reciprocity* (CR) que é analisada para um certo nó x da seguinte forma:

$$CR(x) = \frac{|OS(x) \cap IS(x)|}{|OS(x)|} \tag{1}$$

onde OS(x) representa o conjunto de nós que recebem mensagens de um nó x e IS(x) representa um conjunto de endereços que enviam mensagens para x. Com a escolha

de normalização esta métrica mede a probabilidade de um nó de receber uma resposta de cada um de seus destinatários. Essa métrica permite diferenciar com eficiência spams de não spams, mostrando que e-mails legítimos tipicamente possuem um direcionamento social, ou seja, as mensagens possuem relação bilateral, pois, geralmente são respondidas. Por outro lado, spams não possuem reciprocidade, ou seja, são mensagens unilaterais que atingem uma grande quantidade de destinatários. Por fim, os autores também analisaram a entropia dos fluxos de entrada e saída de cada nó , dada por Shannon (2001):

$$H(x) = \frac{\sum_{y \in OS(x)} -p(y) * log(p(y))}{log(|S(x)|)} \tag{2}$$

onde p(y) é a probabilidade de y receber uma mensagem de x e |S(x)| é o número de elementos chaves no conjunto a ser considerado. Como esperado, foi visto que os spammers se comunicam com seus destinatários com uma variabilidade muito menor (maior entropia) enquanto o tráfego legítimo apresenta menor entropia.

Em busca de maior detalhamento do comportamento dos spammers, Gomes *et al.* (2007) apresentaram uma extensa caracterização de cargas de trabalho de spams. Foram derivados modelos matemáticos para representar a taxa de chegada de spams e o tamanho das mensagens, apresentando comparações com cargas de trabalhos legítimas. Foi visto, por exemplo, que enquanto o envio de mensagens legítimas exibe padrões temporais diários e semanais característicos, com picos em determinados momentos do dia e da semana, o envio de spam não exibe nenhuma diferença significativa em termos de volume ao longo do período analisado. Pode-se perceber que este resultado encontra apoio no estudo de Barabasi (2005), que mostra o envio de e-mail em rajadas.

Além da necessidade de entender o comportamento de spammers para entender e pesquisar formas de contê-los, é interessante saber também como os spammers vêm se comportando ao longo do tempo. O trabalho de Pu e Webb (2006) faz uma análise acerca da evolução temporal das técnicas de construção das mensagens enviadas por spammers, avaliando as técnicas que os spammers utilizam para construir as mensagens. Essas técnicas foram definidas a partir de características identificadas pelo filtro *antispam* utilizado (APACHE, 2010). Os autores mostraram que, ao longo do tempo, algumas técnicas de ofuscação deixam de ser usadas devido a fatores como correção na segurança de programas, mudando assim o ambiente alvo.

Levando em conta este comportamento dinâmico dos spammers, Guerra *et al.* (2010) em extensão ao estudo de Pu e Webb (2006) avalia filtros *antispam* para a análise de tendências de spam, pois, eles são os agentes que podem forçar os spammers a mudar

suas táticas. Além disso, os filtros também evoluem com o tempo e podem apresentar diferentes pontos de vista dos spams. Para esse trabalho foram utilizados filtros antigos e recentes do *Open Source filter Spam Assassin* (APACHE, 2010) para comparar spams dos últimos 12 anos. Os resultados apresentam uma visão geral da natureza dinâmica dos spams nos últimos 12 anos e também mostram que técnicas de spammers mudam a medida que filtros começam a detectá-las. Tal informação pode ter grande importância, pois, auxilia a identificação do comportamento malicioso de usuários através do fluxo de e-mails dos filtros *antispam*.

A interminável batalha entre spammers e anti-spammers é uma característica marcante do problema do spam, conhecida como *spam arms race* (PAULSON, 2005), em que ambos evoluem ao mesmo tempo tentando se sobrepor à força do outro. Por isso, um esforço contínuo para entender como spammers geram, distribuem e disseminam suas mensagens pela Internet é necessário, para manter ou mesmo melhorar a efetividade das técnicas de combate so spam.

2.4 Modelagem de Spammers através de Redes Complexas

Quando um conjunto de vértices são ligados através de um certo número de ligações, e não levando em consideração outro tipo de aspectos, ou seja, os nós da rede sempre possuem a mesma definição, estamos perante a um exemplo mais simples de uma rede. No entanto, estas podem ser mais complicadas. Podem, por exemplo, haver mais do que um tipo de nodos na rede, ou mais do que um tipo de ligações.

Portanto, uma rede complexa é definida em Easley e Jon (2010) como uma rede que possui uma topologia com características específicas, tais como, alto coeficiente de agrupamento, caudas pesadas em distribuições de probabilidade e reciprocidade. No presente trabalho foram utilizadas algumas métricas de redes complexas tais como, popularidade e conectividade, com o propósito de se compreender algumas dimensões do comportamento dos usuários de e-mail.

De acordo com Easley e Jon (2010), a popularidade dos nós uma rede complexa pode ser representada por uma lei de potência (NEWMAN, 2005) e pode ser modelada utilizando a distribuição *Zipf-like*, onde $\alpha > 0$ e C é uma constante de normalização (KLUCKHOHN, 1950).

$$Prob(acessarumobjetoi) = C/i^{\alpha}w \tag{3}$$

Quando uma função decresce a medida que o valor de α cresce, esta função segue uma lei de potência. Por exemplo, se poucos usuários têm alta frequência de utilização de uma rede, e quanto mais esta frequência de utilização é reduzida, o número de usuários aumenta. Ou seja, mostra que poucos usuários utilizam muito os recursos da rede. Logo, a métrica de popularidade foi selecionada para este estudo com o propósito de identificar usuários destinatários "foco" de spams, ou seja, se de fato a frequencia de utilização da rede, no caso, a recepção de spam está concentrada em poucos usuários.

Como pode ser visto em Clauset, Shalizi e Newman (2009), as curvas das distribuições são representadas por uma lei de potência que pode ser analisada a partir da variação dos valores do expoente α. Ou seja, a variação do expoente α pode representar mudanças nas curvas das distribuições. Com isso, este trabalho também utiliza a teoria de lei de potência para analisar de acordo com a variação das distribuições de probabilidade o que acontece com a rede de spam quando o endereço de e-mail dos usuários que receberam uma grande quantidade de spams são renomeados, removidos ou ignorados.

Segundo Newman (2003) o grau de um nó da rede significa o número de conexões que um nó possui com outros nós da rede. Neste trabalho, a conectividade de um remetente (spammer) foi determinada pelo número de usuários que ele/ela pode atingir diretamente, ou seja, está relacionado com a noção de grau do nó. Assim, a conectividade foi analisada somente para os remetentes de spam, pois, como visto na Seção 2.3 as mensagens de spam não têm reciprocidade.

Através dessas métricas foi possível identificar a existência de *heavy users* que enviam muitos e-mails e recebem a maior parte dos spams (ou seja, os usuários mais "populares"). Acredita-se que esses usuários podem prejudicar a gestão de segurança de e-mail e o desempenho da rede por causa da grande quantidade de spams relacionados a eles (PATHAK; JAFRI; HU, 2009). Contudo, ao identificar quem são os *heavy users* pode haver uma grande contribuição para os provedores de e-mails que conhecerão exatamente quais são os usuários que "congestionam" a chegada de e-mails.

Este trabalho utiliza as teorias citadas acima, juntamente com uma metodologia de caracterização do comportamento de usuários de e-mail, para identificar e analisar os usuários "foco" de spam entre os remetentes e destinatários em estudo. Na visão do provedor, a constatação de usuários que recebem muito spams e e-mails e a identificação do comportamento desses usuários pode contribuir com um melhor gerenciamento das contas de usuários de correio eletrônico de um provedor de serviços.

3 METODOLOGIA DE CARACTERIZAÇÃO

Este capítulo apresenta a metodologia de caracterização que delineia o processo de análise do comportamento dos usuários de e-mail, quantificando e qualificando os registros dos *datasets* gerados pelo filtro de spam de um provedor de serviços de correio eletrônico e os registros do *dataset* de e-mails coletado desse mesmo provedor. Entender as características do comportamento dos remetentes e destinatários de spams, com ênfase na identificação dos destinatários, é uma tarefa que pode contribuir para o desenvolvimento e evolução de técnicas para o gerenciamento de contas de usuários de um provedor, possibilitando assim estabelecer uma melhoria nos serviços de e-mails.

A caracterização dos dados neste trabalho foi dividida em duas etapas, pois, existem duas cargas de trabalho que foram coletadas de um mesmo provedor. No Quadro 1 pode ser visualizado a divisão das cargas de trabalho.

Quadro 1 - Divisão das Cargas de Trabalho

	Carga de Trabalho 1	**Carga de Trabalho 2**	
Datasets	*Dataset* de Spam 1	*Dataset* de Spam 2	*Dataset* de E-mail
Período	Jul/10 a Ago/10	Set/10 a Jun/11	Jul/10 a Jun/11

Fonte: Elaborado pelo autor

Inicialmente o conjunto de dados da carga de trabalho 1, foi gerado na infraestrutura de um provedor de e-mails de uma organização privada através do filtro *antispam* denominado "*InterScan Messaging Security Suite 7.0 for Windows*" (TREND-MICRO, 2007). Este filtro foi desenvolvido pela empresa *Trend Micro* a qual possui grande conceito em segurança na troca de informações digitais (NSS-LABS, 2010). Essa carga de trabalho nomeada como "*Dataset* de Spam 1", contém o tráfego de e-mails que chegaram ao provedor e foram considerados maliciosos (ou não legítimos) e, portanto, foram bloqueados pelo filtro de spam. O conteúdo do *Dataset* de Spam 1 foi coletado por um período de 2 meses (julho e agosto de 2010) e possui informações tais como: os remetentes e destinatários das mensagens, IPs e domínios dos usuários, data e hora e classificação do spam.

A carga de trabalho 2, possui o *Dataset* de spam 2 o qual foi gerado no mesmo provedor de e-mails através do mesmo filtro *antispam* e representa a evolução da carga

de trabalho anterior. Ou seja, foram coletados os dados de setembro de 2010 a junho de 2011. Com isso, no total existe um conjunto de dados coletados durante um ano (julho de 2010 a junho de 2011) contendo as mesmas informações do *Dataset* de Spam 1 descritas anteriormente. Esta segunda carga de trabalho foi caracterizada com propósito de apresentar a evolução temporal das principais características encontradas na primeira carga de trabalho de 2 meses.

Além disso, a carga de trabalho 2 também contém todos os e-mails diários enviados e/ou recebidos pelos usuários deste provedor, este *dataset* foi nomeado como "*Dataset* de E-mail". O *Dataset* de E-mail possui os dados do período de 1 ano (julho de 2010 a junho de 2011) e contém informações tais como os remetentes e destinatários das mensagens, data e hora. É válido ressaltar que os dados foram anonimizados pelo administrador do serviço e, portanto, não é possível identificar os usuários na sociedade. Além disso, estes dados estão protegidos por um *Acordo de Privacidade* que não nos permite aprofundar algumas análises. Devido ao grande volume de dados, as duas cargas de trabalho utilizadas foram organizadas por mês afim de viabilizar as análises aqui realizadas.

Para melhor visualizar a estrutura da metodologia aplicada deste trabalho a Figura 1 apresenta um esquema que organiza as etapas que foram seguidas para realizar a caracterização das cargas de trabalho. Em seguida, é apresentado com maior detalhe o processo de caracterização dos remetentes e destinatários de spams e e-mails.

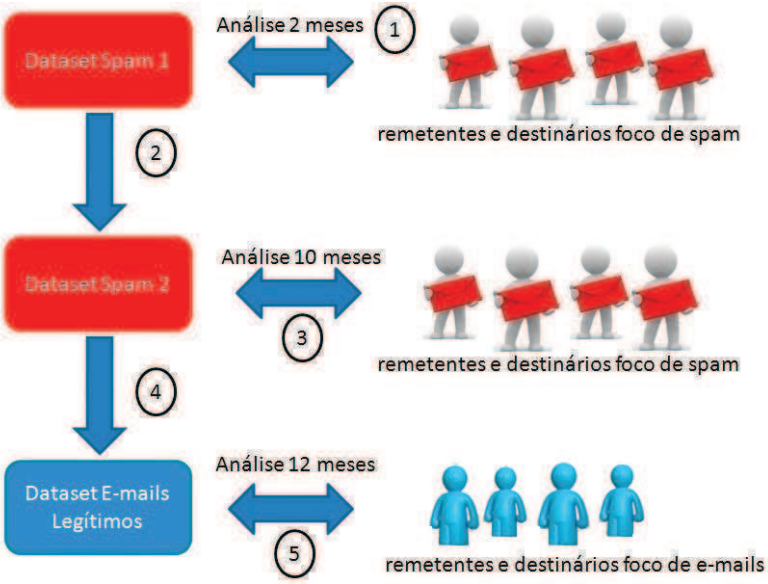


Figura 1: Visão Geral da Metodologia

Fonte: Elaborada pelo autor

De posso do *Dataset* de Spam 1, o primeiro passo 1 foi realizar a caracterização do comportamento dos usuários remetentes e destinatários de spam dos 2 primeiros meses. Para isso, utilizou-se de uma linguagem de programação que permitiu realizar a exploração dos dados. O primeiro passo da análise (1) consistiu na validação dos dados presentes nas cargas de trabalho. Através de um *script* verificou-se se cada registro contido no *Dataset* de Spam 1, de fato, possui os campos relacionados anteriormente (remetentes e destinatários das mensagens, IPs e domínios dos usuários, data e hora e classificação do spam). Além disso, foi verificado a validade dos campos referentes aos remetentes e destinatários, por exemplo, obedecendo os padrões de privacidade todos os registros devem estar no formato "user-Codigo@dominio-Codigo".

Após a validação inicial, o segundo passo foi organizar os registros para iniciar a contagem dos dados afim de obter uma melhor visão da carga de trabalho. Iniciou-se pela contabilização dos remetentes e destinatários distintos em cada um dos 2 meses. Para isso, foram utilizados dois *scripts* que a partir do campo remetentes e do campo destinatários, respectivamente, agrupam os registros semelhantes em uma única linha, ou seja, um único registro.

Os remetentes foram identificados através dos IPs *Senders* contidos no campo IP de cada registro, e os destinatários foram identificados pelos endereços de e-mails contidos no campo *Recipients*. Os remetentes foram identificados através de seus IPs devido ao seu comportamento dinâmico (vide Capítulo 2). Com isso, a saída de cada um dos *scripts* retorna a quantidade de remetentes de destinatários distintos respectivamente, além da quantidade de spams que cada remetente enviou e que cada destinatário recebeu e o total de spams. O Quadro 2 apresenta valores fictícios para demonstrar a saída do *script* que contabiliza a quantidade de destinatários distintos. Vale ressaltar que a saída do *script* que contabiliza os remetentes possui o mesmo formato apresentado no Quadro 2.

Quadro 2 - *Script* de Contabilização de destinatários distintos

Destinatários Distintos	**# Spams Recebidos**
user-1@dominio19.com.br	100.164
user-2@dominio15.com.br	47.634
user-3@dominio12.com.br	14.922
TOTAL SPAMS	162.720

Fonte: Elaborado pelo autor

O mesmo raciocínio apresentado para contabilizar os usuários distintos também foi utilizado nos *scripts* para contabilizar a quantidade de domínios distintos em que cada remetente e destinatários está associado. Logo, houve um *script* para contagem dos

domínios referentes aos remetentes e outro *script* para contabilizar os domínios referentes aos destinatários. Os domínios semelhantes foram agrupados em um único registro, sendo assim, o total de registros presentes na saída do *scripts* totaliza a quantidade de domínios distintos durante cada mês. Além disso, foi possível verificar se os domínios se repetem entre os meses.

Em seguida, iniciou-se a organização da carga de trabalho 2 referente ao passo 2 da Figura 1. Como apresentado, essa carga de trabalho 2 possui o *Dataset* de Spam 2 que contém os dados referentes aos 10 meses subsequentes ao *Dataset* de Spam 1 citado no passo 1. Portanto, o passo 3 representa a análise da evolução temporal do comportamento dos usuários remetentes e destinatários de spams durante 12 meses. Ou seja, utilizou-se *scripts* semelhantes aos utilizados na análise dos remetentes e destinatários nos 2 primeiros meses (*Dataset* de spam 1) afim de verificar se os padrões e características dos usuários apresentados no período de 2 meses permaneceram constante durante os 10 meses seguintes, .

Ao concluir a caracterização dos usuários dos *Datasets* de Spam, foi iniciada a organização do *Dataset* de E-mail (passo 4) o qual possui os dados dos usuários que receberam e/ou enviaram e-mails considerados legítimos no mesmo período de 12 meses. Então, com base nos mesmos parâmetros utilizados para a contabilização dos remetentes e destinatários de spam, realizou-se a caracterização dos usuários de e-mails legítimos no período de 12 meses (passo 5).

Em seguida, através das características relevantes dos usuários de spam e dos usuários de e-mails, buscou-se identificar a relação entre esses usuários, ou seja, foi realizada uma caracterização mais detalhada comparando o comportamento entre os usuários de spams e os usuários de e-mails legítimos. Por exemplo, foi verificado se os principais destinatários de spam (identificados na caracterização dos *Datasets* de Spam) são usuários assíduos ou não, ou seja, se eles enviam muitos ou poucos e-mails por dia. Para o provedor, a identificação de usuários que recebem muito spams e e-mails e a caracterização do comportamento desses usuários pode auxiliar a detecção, por exemplo, de contas desativadas.

Após a contabilização geral de ambas cargas de trabalho, foram realizadas a análise da qualitativas nos dados dos usuários presentes nos *Datasets* de Spam e no *Dataset* de E-mail. Analisou-se a popularidade e da conectividade (métricas de redes complexas), com o propósito de se compreender algumas dimensões do comportamento dos usuários remetentes e destinatários de spams e de e-mail. Entretanto, as análises foram realizadas

com base, principalmente, na popularidade dos destinatários de mensagens eletrônicas. Em busca de identificar possíveis destinatários "foco" de recepção de spam.

O processo detalhado acima, apresenta uma visão geral da metologia aplicada neste trabalho referente a Figura 1. Porém, durante o processo de contabilização houve outras análises importantes na caracterização do comportamento dos remetentes e destinatários de spams e e-mails. Por exemplo, o campo classificação do spam presente nos registros dos *Dataset* de Spam 1 também é relevante, pois é responsável por informar a gravidade do spam, de acordo com configurações pré-definidas pelo filtro *antispam* da *Trend Micro*.

Portanto, durante a organização dos registros dos *Dataset* de Spam 1, foram armazenados também os valores máximo, mínimo e médio do *Trend Score* dos spams trafegados na rede. A partir desses valores foi possível identificar a relação entre a quantidade de spams recebidos e enviados pelos usuários com o valor médio do *Trend Score*, o que representa a gravidade do spam que foi filtrado. Com isso é possível identificar usuários que recebem ou disseminam spams considerados mais graves e que, por isso, podem causar um dano maior tanto ao usuário destinatário da mensagem quanto ao provedor de serviços de correio eletrônico. A Figura 2 apresenta a estrutura do campo classificação presente nos registros dos *Dataset* de Spam 1 analisado. Em seguida, é apresentada a definição de cada campo desta classificação:

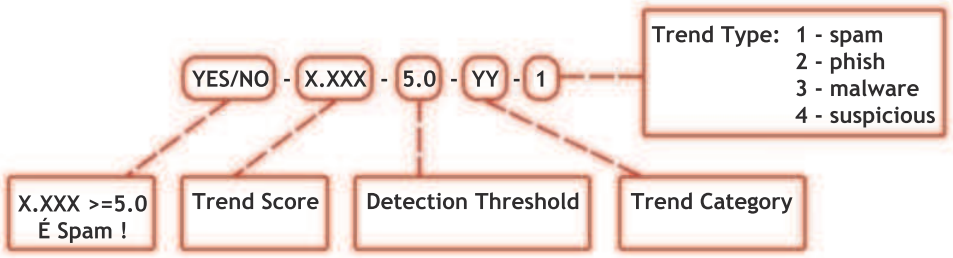


Figura 2: Campo Classificação do Spam

Fonte: Elaborada pelo autor

a) O primeiro campo informa se o e-mail foi considerado spam (*Yes* ou *No*).

b) *Trend Score*: representa a "pontuação" do spam utilizando regras pré-definidas.

c) *Detection Threshold*: corresponde ao *Administration Console Settings* configurado para o filtro de spam; este pode possuir os níveis baixo (4.0), médio (5.0) e alto

(6.0); para a coleta deste *Dataset* de Spam 1 foi utilizada a configuração com o nível médio.

d) *Trend Category*: define qual categoria o spam pertence; não é utilizado para esta coleta, ou seja, todos spams são de uma mesma categoria.

e) *Trend Type*: tem o valor 1 (spam) como padrão; os outros possíveis valores são: 2-*phish*, 3-*malware* e 4-*suspicious*; registros com estes últimos valores não foram capturados nessa coleta.

Segundo as regras definidas no *Administration Console Settings* do filtro de *antispam*, sempre que o *Trend Score* for maior ou igual ao *Detection Threshold* temos um e-mail considerado spam. Com essa classificação dos spams foi possível verificar quais são os e-mails mais "graves", ou seja, aqueles e-mails que possuem maior *Trend Score*.

3.1 Seleção e Classificação dos dados das Cargas de Trabalho

No Capítulo 2, foi visto que os estudos recentes buscam caracterizar o comportamento de spammers afim de obter maior conhecimento para aprimorar técnicas de bloqueio de spams. Entretanto, além da análise dos usuários remetentes de spam, iremos apresentar também a análise dos destinatários de spams.

Conhecer o comportamento dos usuários destinatários de spam pode ser interessante para o provedor de e-mails que conhecerão os possíveis usuários que atraem uma maior quantidade de mensagens não desejadas. Logo os usuários destinatários de spams ou e-mails são foco deste trabalho e serão analisados mais detalhadamente, buscando identificar o motivo desta concentração de mensagens eletrônicas em tais usuários. Com base nessas informações, para as análises mais detalhadas dos *Datasets* de Spam 1 e 2 de ambas as Cargas de Trabalho, foram considerados dois pontos de vista:

a) Remetentes de spams: registros agrupados por cada IP *sender* distinto, contabilizando a quantidade de destinatários para cada IP; este conjunto de dados representa todos remetentes de spams.

b) Destinatários de spams: registros agrupados por cada destinatário distinto, contabilizando a quantidade de spams para cada destinatário; este conjunto de dados representa todos os destinatários de spams.

Com o propósito de obter uma melhor visualização dos dados e identificação das características dos usuários, na análise inicial do *Dataset* de Spam 1 (Carga de Trabalho 1)

os remetentes e destinatários de spams foram estudados separados por semanas. Para isso, foram selecionadas 4 semanas entre julho e agosto de 2010 consideradas quantitativamente relevantes para o estudo, ou seja, as semanas em que houve uma maior quantidade de e-mails trocados entre os usuários desse tipo de serviço.

Para a análise do *Dataset* de E-mail da Carga de Trabalho 2, os registros foram agrupados pelos remetentes e destinatários distintos (usuários do provedor de e-mails), contabilizando a quantidade de e-mails que estes enviaram e/ou receberam. Este conjunto de dados representa todos os usuários que receberam ou enviaram e-mails desse provedor no período estudado. Com isso, caracterizou-se o comportamento dos destinatários de spams em conjunto com o comportamento dos usuários de mensagens legítimas. Assim, foi possível verificar a relação entre os usuários dessas duas cargas de trabalho.

Na seção a seguir, são apresentados os resultados encontrados a partir da metodologia aplicada nesta pesquisa. Será apresentada a análise da evolução temporal dos destinatários de spams, que foi realizada através do cálculo das distribuições de probabilidade acumulada dos usuários durante os 10 meses, afim de identificar como permanece a popularidade dos usuários destinatários durante o período de 1 ano. Além disso, no *Dataset* de E-mail, foram identificados os usuários do provedor que mais enviam e/ou recebem e-mails através da contabilização dos dados. Esses usuários foram associados aos destinatários considerados "foco" de spam afim de encontrar características que justifique esta grande quantidade de spams recebidos no período estudado.

4 RESULTADOS

Este capítulo apresenta e discute os principais resultados encontrados na caracterização dos remetentes e destinatários de spams e de e-mails em estudo com foco na análise dos usuários destinatários. Inicialmente, foi realizada a contabilização e análise dos dados separadamente para os remetentes e destinatários e para cada carga de trabalho. Na próxima seção é apresentada a visão geral da contabilização das cargas de trabalho. Em seguida, serão apresentadas as análises dos remetentes e destinatários e spam do *Dataset* de Spam 1 referente a Carga de Trabalho 1 e a caracterização do *Dataset* de Spam 2 referente a Carga de Trabalho 2. A caracterização do *Dataset* de Spam 2 apresenta a evolução das análises das principais características encontradas na caracterização dos dados durante o 2 meses iniciais. Ou seja, verifica-se a evolução temporal dos resultados encontrados durantes os 10 meses seguintes. Ao final, será apresentada a caracterização do *Dataset* de E-mail e a relação com os resultados encontrados nos *Datasets* de Spams.

4.1 Visão Geral da Carga de Trabalho 1

Como visto no capítulo 3, no primeiro momento foi analisada a carga de trabalho 1 na qual foi realizada uma contabilização geral do conteúdo do *Dataset* de Spam 1. No período de 2 meses consecutivos, aproximadamente 6 milhões dos e-mails que chegaram ao provedor foram considerados maliciosos e, por isso, foram bloqueados pelo filtro de spam. Esses e-mails contêm cerca de 400 mil remetentes distintos, os quais estão relacionados a aproximadamente 37 mil domínios diferentes. A Tabela 1 apresenta uma visão geral da distribuição dos remetentes e destinatários de spam durantes os 2 meses.

Tabela 1: **Remetentes e destinatários de spam - Carga de Trabalho 1**

Carga de Trabalho 1 - *Dataset* de Spam 1					
Meses	**Remetentes**		**Destinatários**		**# E-mails**
	# Usuários	**# Domínios**	**# Usuários**	**# Domínios**	
Julho	285.028	25.799	4.129	18	2.404.025
Agosto	139.771	20.853	4.070	18	3.358.509
					5.762.534

Fonte: Elaborado pelo autor

Pode ser observado de acordo com a quantidade de remetentes e domínios uma quantidade elevada de spammers distribuídos em poucos domínios. Tais valores, podem ser justificados por estudos anteriores como Gomes *et al.* (2007) e Guerra *et al.* (2010) que apontam a existência de um comportamento dinâmico dos spammers, pois, eles normalmente alteram a identificação dos remetentes ou dados do corpo da mensagem, mesmo permanecendo no mesmo domínio.

O provedor de e-mail possui cerca de 4.000 contas de usuários distintos, sendo estes distribuídos nos 18 domínios diferentes gerenciados pelo provedor de serviços. Tendo em vista que tais usuários em média receberam aproximadamente 1.000 spams durante o período de 2 meses da coleta do *Dataset* de Spam 1, foi possível verificar a existência de usuários foco de spam, ou seja, usuários que recebem uma grande quantidade de mensagens não solicitadas em comparação aos outros usuários remetentes e destinatários de spam. Particularmente, existe um único destinatário que recebeu mais de 100 mil spams no período, enquanto outros receberam apenas uma ou duas mensagens classificadas como spam.

Tais remetentes e destinatários podem ser responsáveis por prejudicar o desempenho de provedores de e-mails, uma vez que uma grande quantidade de spams se concentram em um número restrito de usuários destinatários. Contabilizando a quantidade de domínios nos 2 meses, é possível observar que dos 37 mil domínios distintos dos remetentes, cerca de 10 mil domínios se repetem entre os meses de julho e agosto de 2010.

4.2 Visão Geral da Carga de Trabalho 2

Após a caracterização da carga de trabalho 1, foram contabilizados os *Datasets* da carga de trabalho 2. Foi realizada uma contabilização geral do conteúdo do *Dataset* de Spam 2 e do *Dataset* de E-mail. Na Tabela 2 é apresentada uma visão geral dos remetentes e destinatários de spam no *Dataset* de Spam 2.

Para o *Dataset* de Spam 2 durante o período de 12 meses, pode ser visto na Tabela 2 que aproximadamente 20 milhões dos e-mails que chegaram ao provedor foram considerados maliciosos e, por isso, foram bloqueados pelo filtro *antispam*. Esses e-mails contêm cerca de 2 milhões de remetentes, os quais estão relacionados a aproximadamente 158 mil domínios. Pode ser observado que o comportamento dinâmico dos remetentes como vimos nos primeiros 2 meses analisados no *Dataset* de Spam 1, prevalece durante os outros 10 meses, isso pode ser concluído de acordo com a quantidade de remetentes e domínios, a proporção de 1 domínio para cada 13 remetentes distintos, apresentando uma grande quantidade de spammers distribuídos em poucos domínios.

Tabela 2: **Remetentes e destinatários de spam - Carga de Trabalho 2**

Carga de Trabalho 2 - *Dataset* de Spam 2					
Mes/Ano	**Remetentes**		**Destinatários**		**# E-mails**
	# Usuários	**# Domínios**	**# Usuários**	**# Domínios**	
Set/2010	273.020	18.290	4.243	18	2.397.600
Out/2010	138.715	16.200	4.053	18	1.853.430
Nov/2010	236.605	15.640	4.060	18	2.193.334
Dez/2010	260.748	14.982	5.181	19	2.332.453
Jan/2011	293.608	13.609	5.060	20	2.259.342
Fev/2011	103.799	13.335	5.077	22	1.578.987
Mar/2011	92.704	14.475	5.300	19	1.644.344
Abr/2011	104.100	14.187	5.188	20	1.707.125
Mai/2011	100.307	13.405	5.228	25	1.867.562
Jun/2011	89.042	14.113	5.367	17	1.703.342
				Total de E-mails	**19.537.519**

Fonte: Elaborado pelo autor

Quanto aos destinatários de spam, como os dados foram coletados do mesmo provedor de e-mail, a quantidade de contas de usuários não é muito diferente da quantidade de contas do *Dataset* de Spam 1, possuindo aproximadamente 5.000 contas de usuários distintos. Esses usuários estão distribuídos em 20 domínios diferentes gerenciados pelo provedor de serviços de e-mail. Foi possível observar novamente a existência de usuários foco de spam nos 10 meses referentes ao período de setembro/2010 a Junho/2011, repetindo o padrão de concentração de spams em poucos usuários destinatários como observado nas análises do *Dataset* de spam 1, nos 2 primeiros meses estudados.

Para o *Dataset* de E-mail, também foi realizada uma contabilização geral do conteúdo semelhante aos *Datasets* de spam. A Tabela 3 pode ser visto melhor os valores encontrados.

Pode ser observado que foram enviados ou recebidos pelos usuários do provedor aproximadamente 10 milhões de e-mails no período de 1 ano. Esses e-mails contêm cerca de 100 mil usuários remetentes distintos incluindo os usuários do provedor, os quais estão relacionados a aproximadamente 15 mil domínios diferentes. Quanto aos destinatários dos e-mails, pode ser observado a existência de em média 80 mil usuários destinatários distintos por mês, mostrando que os usuários remetentes desse provedor enviam muitos e-mails para uma grande quantidade de destinatários diferentes espalhados em média entre 10 mil domínios distintos. Entretanto, seguindo o objetivo deste trabalho, a análise foi focada somente nos e-mails recebidos e/ou enviados entre os usuários do provedor de e-mail (aproximadamente 5 mil usuários).

Tabela 3: **Remetentes e destinatários de e-mail - Carga de Trabalho 2**

Carga de Trabalho 2 - *Dataset* de Email					
Mes/Ano	**Remetentes**		**Destinatários**		**# E-mails**
	# Usuários	**# Domínios**	**# Usuários**	**# Domínios**	
Jul/2010	101.159	13.834	58.922	10.488	718.564
Ago/2010	118.000	14.304	83.129	10.705	989.850
Set/2010	65.900	10.305	58.275	6.749	523.107
Out/2010	87.968	11.905	64.089	6.833	756.708
Nov/2010	87.862	11.891	60.346	7.060	545.003
Dez/2010	104.130	11.989	48.687	6.497	497.852
Jan/2011	118.796	12.862	39.718	5.725	637.742
Fev/2011	120.266	13.587	71.018	7.523	958.569
Mar/2011	117.774	14.002	110.227	21.211	1.033.135
Abr/2011	126.273	14.101	73.404	7.942	1.069.526
Mai/2011	144.989	15.578	88.305	11.402	1.299.203
Jun/2011	138.143	15.521	79.571	8.067	1.283.891
				Total de E-mails	**9.011.080**

Fonte: Elaborado pelo autor

Foi possível observar ainda a existência de usuários "foco" de envio/recepção de e-mails, ou seja, usuários que enviam ou recebem uma grande quantidade de e-mails em comparação aos demais usuários. Particularmente, existe um único remetente que enviou mais de 100 mil e-mails por mês, enquanto outros enviaram em torno de 10 mensagens eletrônicas. Uma vantagem em encontrar tais dados é identificar se a conta de um usuário que enviou ou recebeu milhares de e-mails é uma conta ativa ou uma conta inutilizada, que apenas recebe e-mails automáticos. Além disso, é importante verificar se tal usuário está presente entre os usuários foco de spam, pois o grande fluxo de e-mail não importantes enviados ou recebidos somados a grande quantidade de spams recebidos deste usuários pode causar prejuízos para o provedor de e-mail.

4.3 Remetentes e Destinatários de Spams - *Dataset* de Spam 1

Com o intuito de entender a propagação dos spams entre os usuários de troca de e-mails, a caracterização dos registros dos usuários foi realizada considerando os dois pontos de vista (Remetentes de spams e Destinatários de spams) citados na Seção 3.1. Nas subseções a seguir são apresentados os resultados encontrados na caracterização dos remetentes e destinatários de spam do *Dataset* de Spam 1.

4.3.1 Análise dos Usuários Remetentes de Spam

A caracterização dos remetentes foi realizada para cada uma das 4 semanas selecionadas. Contabilizando os spams enviados em cada semana e relacionando-os aos

remetentes responsáveis, na semana 1 cerca de 4% dos remetentes foram responsáveis pelo envio de 50% dos spams, sendo 5% na semana 2 e 6% na semana 3 e 4, apresentando uma média de 5% durante as 4 semanas. Na Tabela 4 pode ser visto os valores absolutos dos percentuais citados acima.

Tabela 4: **Visão geral dos remetentes de spam durante as semanas**

Semana	# **IPs Remetentes**	# **Heavy Senders (enviam 50% spams)**	% **Remetentes que enviam 50% dos spams**
1	3.404	150	4,41%
2	12.167	558	4,60%
3	9.369	548	5,87%
4	11.975	868	7,27%

Fonte: Elaborado pelo autor

Observa-se que a quantidade de remetentes responsáveis pelo envio de uma grande quantidade de spams não varia muito de uma semana para outra. Tal fato pode ser justificado pela contabilização dos dados ter sido realizada com base no campo IP dos remetentes de spam. Como visto no Capítulo 2 nas pesquisas de Gomes *et al.* (2007) e Guerra *et al.* (2010), spammers possuem um comportamento dinâmico. Porém, ao analisar o volume de tráfego gerado pelo IP foi possível identificar usuários com remetentes distintos partindo de um mesmo IP em semanas diferentes.

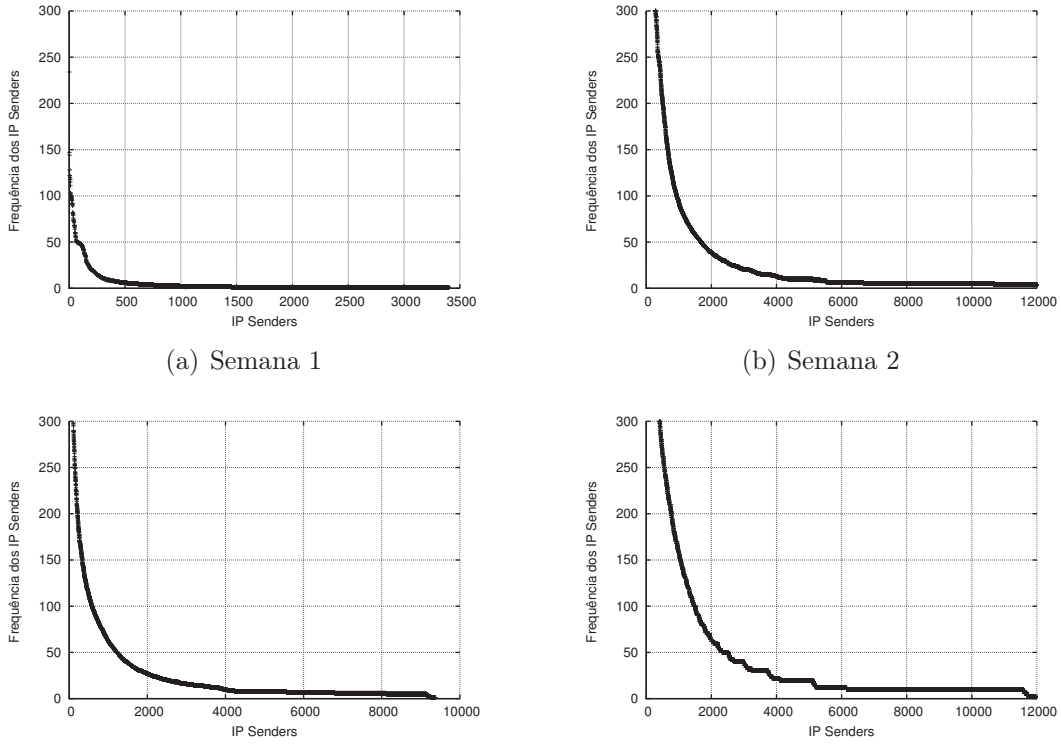
Para analisar a conectividade dos spammers foram contabilizados os e-mails trocados desses com os usuários. Verificou-se que para o período analisado existe uma quantidade alta de remetentes de spam (400 mil) para um número relativamente baixo de destinatários (4 mil). Avaliando a quantidade de spams enviados para os usuários finais (aproximadamente 6 milhões de spams), é possível identificar se tais spammers possuem alta conectividade entre os usuários destinatários.

Para isso, verificou-se que dentre os 6 milhões de spams bloqueados pelo filtro, estes se espalham regularmente entre os destinatários, onde em média os usuários destinatários recebem cerca de 1.700 e-mails por semana. Isso mostra que os remetentes de spams atingem constantemente todos os destinatários. Entretanto, foi visto a existência de usuários que concentram mais spams que outros, chegando a um máximo de 100 mil spams para único usuário destinatário, tais usuários podem ser considerados usuários foco de spam.

Para analisar a popularidade dos usuários foram calculadas as PDFs[1] dos usuários separados por semanas. A Figura 3 apresenta a disposição das curvas das PDFs dos IPs Remetentes de spam. Pode ser visualizado nessas PDFs um comportamento típico de

[1] *Probability Distribution Frequency (PDF).*

uma lei de potência (NEWMAN, 2005), onde poucos remetentes enviam spams para uma grande quantidade de usuários finais, enquanto a maioria dos spammers envia mensagens maliciosas para poucos destinatários. Em outras palavras, uma quantidade bem menor de remetentes de spams têm alta popularidade. Observa-se que a curva da distribuição está sempre bem acentuada e próxima ao eixo y, mostrando que os remetentes de spams se concentram em poucos usuários, mais precisamente menos que 2 mil spammers. Com isso, conclui-se que o envio de spam de fato se concentra em poucos remetentes, mostrando uma maior popularidade de certos spammers que podem ser considerados "foco" da disseminação de mensagens não solicitadas.



(a) Semana 1

(b) Semana 2

(c) Semana 3

(d) Semana 4

Figura 3: PDFs dos remetentes de spam durante as 4 semanas

Para melhor visualizar tal fato, foram selecionados dentre os remetentes aqueles que enviaram 50% dos spams para cada semana selecionada. Esses usuários foram denominados como *Heavy Spam Senders*. É possível ver na Tabela 4 que mesmo com a quantidade de remetentes aumentando como mostra na semana 2, atingindo aproximadamente 12 mil IPs, o percentual dos que enviam 50% dos spams não é superior a 8%, mostrando que estes IPs podem estar associados a usuários foco de envio de spams.

A descoberta de dados desse tipo, como a concentração de envio de spam em poucos remetentes é útil para possíveis melhorias na rede de correio eletrônico. Ao tratar

tais usuários foco de spam, pode-se evitar o desperdício de recursos para combater os spammers e consequentemente melhorar o desempenho de serviços de e-mail.

4.3.2 Movimentação dos Remetentes de Spam

Como visto no Capítulo 2, os trabalhos apontam um grande dinamismo do comportamento dos spammers Gomes *et al.* (2007), ou seja, os remetentes de spam estão sempre alterando seus IPs ou de alguma forma trocando seus dados, portanto spammers não exibem padrões temporais diários e semanais característicos. Tal característica também está presente nos remetentes de spam analisado neste trabalho. Pode ser visualizada para cada uma das 4 semanas selecionadas para esta pesquisa, a alta movimentação dos spammers. A cada semana os IPs remetentes de spam são alterados continuando poucos spammers com o mesmo IP.

Na Tabela 5 é apresentada a movimentação dos IPs remetentes de spam durante este período de 4 semanas. Os IPs que continuaram representa aqueles usuários remetentes que continuam enviando spam utilizando o mesmo IP de uma semana para a semana seguinte. Os IPs novos são aqueles usuários que na semana anterior não enviou nenhum spam para o provedor utilizando o IP referente a ele, porém enviou mensagem maliciosa com esse IP na semana corrente e os IPs que saíram representa os usuários que enviaram mensagens ilegítimas na semana anterior utilizando um IP e na semana corrente já não utiliza esse IP mais.

Tabela 5: **Evolução Temporal dos remetentes durante as semanas**

Semana	**# IPs que continuaram**	**# IPs que saíram**	**# IPs novos**
1	0	0	0
2	3	145	555
3	147	411	401
4	0	548	868

Fonte: Elaborado pelo autor

Observa-se que a quantidade de IPs novos, ou que saem durante as semanas, é sempre maior que a quantidade de IPs que continuam nas semanas seguintes. Isto pode ser visualizado durante as semanas 2, 3 e com ênfase na semana 4, quando todos 568 IPs saíram, ou seja, deixaram de enviar spams utilizando esses IPs remetentes e 868 novos IPs entraram, ou seja, IPs remetentes que na semana anterior não havia enviado spams. Tais dados mostram a constante alteração dos IPs dos remetentes ao enviarem spams para seus destinatários, comprovando que os spammers constantemente alteram seus IPs de envio em busca de enganar as técnicas e filtros *antispam*.

4.3.3 Análise dos Usuários Destinatários de Spam

A caracterização dos destinatários de spams também foi realizada para cada uma das 4 semanas selecionadas. Ao contabilizar a quantidade de spams enviados para um determinado usuário final, encontrou-se foco de destinatários em cada semana analisada. Na primeira semana, 22% dos destinatários foram alvos de 50% do total de spams, nas semanas 2 e 4, apenas 13% dos destinatários foram alvos deste mesmo percentual de spams enviados, e na terceira semana 12% dos usuários receberam metade dos spams. Na Tabela 6 tal fato pode ser melhor visualizado.

Tabela 6: **Visão geral dos destinatários de spam durante as semanas**

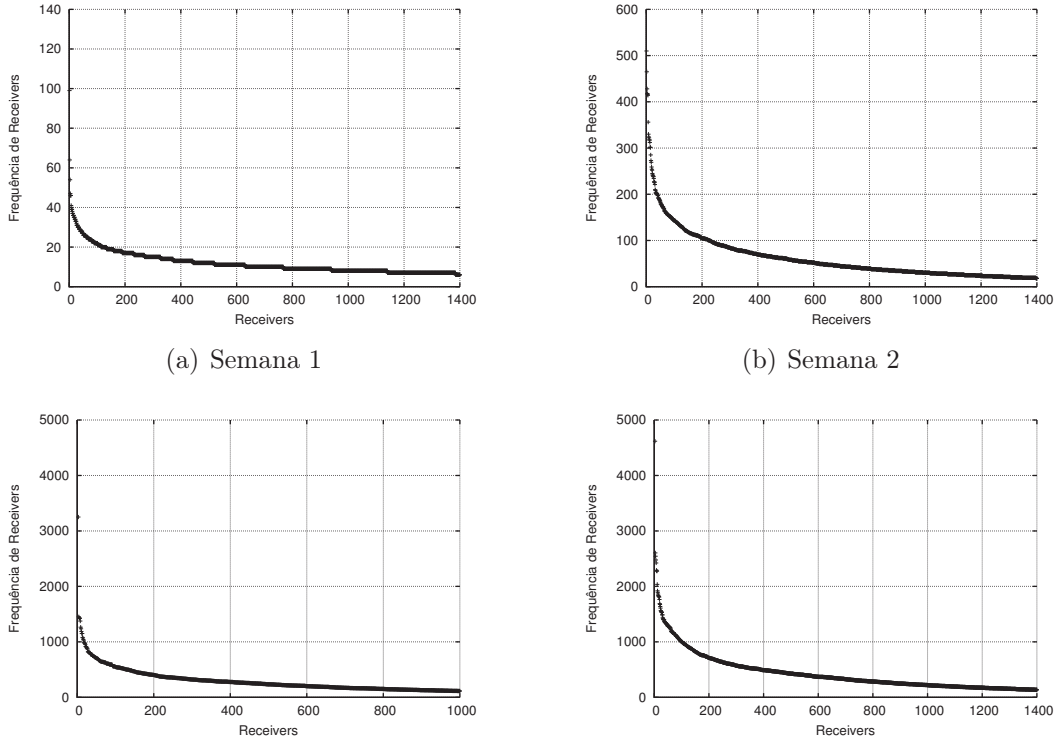
Semana	**Total *Recipients***	**Quantidade Heavy *Recipients* (recebem 50% spams)**	**% *Recipients* recebem 50% dos spams**
1	2.365	150	22,41%
2	3.036	558	13,18%
3	3.163	548	11,70%
4	3.226	868	12,59%

Fonte: Elaborado pelo autor

Os valores mostram uma variação maior ocorrendo da semana 1 para semana 2. Porém, tal valor pode ser justificado devido à semana 1 possuir menor quantidade de usuários finais do que a semana 2, e desta forma, os spams se concentram em um número menor de destinatários. Para as outras semanas (3 e 4) percebe-se que há uma concentração de muitos spams para poucos usuários destinatários. Observa-se que apesar de ter uma quantidade de destinatários maior como mostra na semana 4, o percentual dos usuários que recebem pelo menos 50% dos spams não é superior a 14% nas semanas 2 a 4.

A popularidade de certos destinatários de spam, assim como os remetentes, também se concentram em poucos usuários. A Figura 4 apresenta as curvas PDFs dos destinatários de spams durante as 4 semanas selecionadas. Observa-se que as curvas das distribuições se concentram sempre próximo ao eixo y, o que representa menores quantidades de usuários. Isso mostra uma maior popularidade de certos destinatários entre os usuários alvo de spams.

Assim como nos remetentes analisados na Subseção 4.3.1, as PDFs dos destinatários de spam também apresentam um comportamento típico de uma lei de potência. Isto aponta que poucos usuários receberem muito spam, enquanto a maioria dos usuários destinatários recebem menor quantidade de spams. Pode-se concluir também que poucos destinatários de spam têm alta popularidade entre os IPs Remetentes de spam. Assim



(a) Semana 1

(b) Semana 2

(c) Semana 3

(d) Semana 4

Figura 4: PDFs dos destinatários de spam durante as 4 semanas

como foi feito para os remetentes de spam, estes usuários foram denominados como *Heavy Spam Recipients*.

Analisando pela visão do administrador do provedor, a descoberta de dados desse tipo, como a concentração de envio de spam para poucos destinatários pode ser útil na identificação de usuários que atraem spams. Ao serem identificados e tratados devidamente, poderia facilitar o serviço do provedor de e-mails no bloqueio aos spams que tais usuários finais iriam atrair para suas caixas de entrada. Como consequência, seria possível alcançar um melhor desempenho nos serviços de e-mails, não congestionando o envio de mensagens válidas, como apresentado na Seção 2 no trabalho de (TWINING *et al.*, 2004).

4.3.4 Classificação dos Spams dos Remetentes e Destinatários

Outro fator interessante da análise dos spammers neste estudo é a classificação do spam que foi enviado. Esta classificação, é realizada pelo filtro *antispam* utilizado pelo provedor de e-mails no qual o *dataset* foi coletado. Através desse campo de classificação é possível identificar a gravidade de cada spam enviado ao provedor de mensagens eletrônicas. Como citado anteriormente o capítulo 3, foram armazenados os valores máximos, mínimos e as médias dos *Trend Scores* dos e-mails dos remetentes e destinatários em es-

tudo. Com esses valores verificou-se a relação entre a quantidade de spams recebidos e enviados pelos usuários com o valor médio do *Trend Score*.

Na Tabela 7 são apresentados os valores médios dos *Trend Scores* contabilizados de forma geral. Ela mostra também a média dos *Trend Scores* para os *Heavy* spams *senders* e *recipients* e a média dos *Trend Scores* para "*Light*" spams *senders* e *recipients*, esse último grupo representa os demais usuários que não foram considerados "foco" de spam.

Tabela 7: **Média do *Trend Score* para os usuários**

Semana	**Média Geral**		**Média Heavy**		**Média Light**	
	Senders	***Recipients***	***Senders***	***Recipients***	***Senders***	***Recipients***
1	67,244	35,127	737,077	67,163	36,769	25,705
2	5,605	6,297	33,774	7,104	4,250	6,176
3	48,798	8,870	19,880	27,501	5,059	6,415
4	0,041	14,007	3,282	47,657	0,018	9,186

Fonte: Elaborado pelo autor

Pode ser visto que para os *Heavy* spams (*senders e recipients*) a média do *Trend Score* é sempre mais alta, como, por exemplo, a semana 4, em que a média geral do *Trend Score* dos *Recipients* é 14,007 e a média dos *Heavy* e *Light Recipients* são respectivamente 47,657 e 9,186. Tais dados mostram a maior gravidade dos spams recebidos pelos *Heavy Recipients* e enviados pelo *Heavy Senders*.

Este é mais um fator importante entre as características dos remetentes e destinatários deste trabalho, pois como foi visto, a quantidade de *Heavy senders* é pequena (concentra em poucos usuários), mas os spams disseminados por estes usuários são mais graves. Portanto, ao identificar e tratar estes usuários destinatários que recebem spams considerados mais graves e que são usuários foco de spam (*Heavy Recipients*), o desempenho dos serviços de e-mail serão diretamente beneficiados.

4.3.5 Eliminação dos Heavy Spam Recipients

Nos resultados obtidos nas seções anteriores, foi visto que o envio de grande parte dos spams se concentram em uma pequena quantidade de usuários destinatários que foram denominados como *Heavy Spam Recipients*. Esta seção analisa a retirada desses *Heavy Spam Recipients* para cada umas das 4 semanas selecionadas. Foram eliminados os usuários responsáveis por 50% dos spams recebidos e verificou-se o impacto da ausência desses usuários destinatários.

Uma métrica comum utilizada para comparar redes de usuários é o expoente α obtido através da regressão linear de uma distribuição de lei de potência (BENEVENUTO; ALMEIDA; SILVA, 2011). Tal métrica foi utilizada para analisar os usuários de spams,

após a retirada dos *Heavy Spam Recipients*. Aplicou-se a regressão linear para calcular o expoente da distribuição antes e depois da eliminação dos usuários foco de spam. A Tabela 8 apresenta os valores dos expoentes alpha para as distribuições em cada semana analisada.

Tabela 8: **Variação do alpha após eliminar os *Heavy Spam Recipients***

Semanas	**Valor do expoente alpha**	
	Todos Destinatários de Spam	**Após remoção dos *Heavy Recipients***
1	1,77	1,66
2	1,36	1,32
3	1,28	0,86
4	1,25	0,76

Fonte: Elaborado pelo autor

Observando os valores da variação dos expoentes *alpha* ao retirar os *Heavy Spam Recipients*, foi possível verificar que os valores do expoente das leis de potência diminuem em todas as semanas analisadas. Nas semanas 3 e 4 houve uma maior queda no valor do expoente α. Tal fato ocorre devido a essas semanas possuírem uma quantidade maior de destinatários "foco" de spam, pois com a retirada desses usuários destinatários interfere mais na curva da distribuição e, consequentemente, no valor do α. Como pode ser visto em Clauset, Shalizi e Newman (2009) quanto menor for o valor do expoente α da lei de potência em questão, menos forte é o decaimento da cauda e mais grossa será a cauda da distribuição.

Portanto, ao retirar os usuários que recebem grande quantidade de spams (10% do usuários) alterou-se a curva da distribuição de lei de potência suavizando seu decaimento. Isso mostra que ao entender o comportamento de poucos usuários destinatários de spam pode-se obter um ganho no gerenciamento de segurança da rede, uma vez que estes usuários "foco" são responsáveis por uma grande quantidade de spams recebidos pelo provedor de correio eletrônico.

4.4 Remetentes de Destinatários de Spam - *Dataset* de Spam 2

Nesta seção são caracterizados os remetentes e destinatários de spams presentes no *Dataset* de Spam 2 referente a Carga de Trabalho 2. Como apresentado no Capítulo 3, este *dataset* possui os dados de setembro de 2010 a junho de 2011 e apresenta a evolução da carga de trabalho analisada na seção anterior. Porém, nas subseções a seguir a análise é focada em algumas características relevantes para este trabalho, como na popularidade

dos remetentes e destinatários de spam afim de verificar se este comportamento permanece durante os 10 meses subsequentes ao *Dataset* de Spam 1.

4.4.1 Análise dos Usuários Remetentes de Spam

A análise dos usuários remetentes de spam do *Dataset* de Spam 2 foi realizada para cada um dos 10 meses. Os dados foram contabilizados afim de verificar se o envio de maior parte das mensagens não desejadas ao provedor, ocorre por uma quantidade menor de remetentes de spam (percentual baixo de spammers), como foi visto na análise do *Dataset* de Spam 1 apresentado anteriormente. Portanto, a caracterização não foi aprofundada como realizado para os remetentes de spams dos 2 meses iniciais, pois como apresentado no objetivo deste trabalho o interesse maior está nos usuários destinatários.

Foram contabilizados os spams enviados de cada um dos 10 meses e relacionando-os aos remetentes responsáveis. A Tabela 9 apresenta o percentual de spammers que enviaram 50% do total de spammers no período de setembro de 2010 a junho de 2011.

Tabela 9: **Visão geral dos remetentes de spam durante os 10 meses**

Meses	**Total *Senders***	**# Heavy *Senders* (enviou 50% spams)**	**% *Senders* enviam 50% dos spams**
Set/2010	273.020	10.970	4,02%
Out/2010	138.715	707	0,51%
Nov/2010	236.605	6.220	2,39%
Dez/2010	260.748	7.230	2,77%
Jan/2011	293.608	15.307	5,21%
Fev/2011	103.799	796	0,77%
Mar/2011	92.704	802	0,87%
Abr/2011	104.100	951	0,91%
Mai/2011	100.307	900	0,85%
Jun/2011	89.042	580	0,65%

Fonte: Elaborado pelo autor

Pode ser observado que o percentual de spammers que enviam metade dos e-mails maliciosos não ultrapassa 6%, mostrando que o envio de grande parte de spams é realizado por poucos usuários remetentes de spam. Logo, o padrão de menor quantidade de spammers que enviam maior parte das mensagens não desejadas verificado na análise inicial dos 2 primeiros meses, permanece para os 10 meses subsequentes a agosto de 2010.

4.4.2 Análise dos Usuários Destinatários de Spam

A caracterização dos destinatários de spams para o *Dataset* de Spam 2 também foi realizada para cada o período de setembro de 2010 a junho de 2011. Ao contabilizar a quantidade de spams enviados para um determinado usuário final, como visto nos 2

primeiros meses analisados, foi observado novamente "foco" de destinatários de spam para cada um dos 10 meses subsequentes a julho e agosto de 2010.

Confirmando a evolução temporal dessa característica, entre os meses de setembro e novembro de 2010, 13% dos destinatários foram alvos de 50% do total de spams, reduzindo para 11% de dezembro de 2010 a janeiro de 2011. No período de fevereiro de 2011 a junho de 2011, entre 7% e 8% dos usuários receberam 50% dos spams representando uma maior concentração do envio de spams em menor quantidade de destinatários.

Tais valores podem ser visualizados na Tabela 10 que apresenta uma visão geral dos destinatários de spams durante esse período. Os valores mostram uma queda ocorrendo dos meses de setembro a dezembro de 2010 comparados aos meses de março a junho de 2011. Porém, tais valores podem ser justificados devido aos meses de 2010 possuir menor quantidade de destinatários que os meses de 2011, e desta forma, os spams se concentram em um número menor de destinatários.

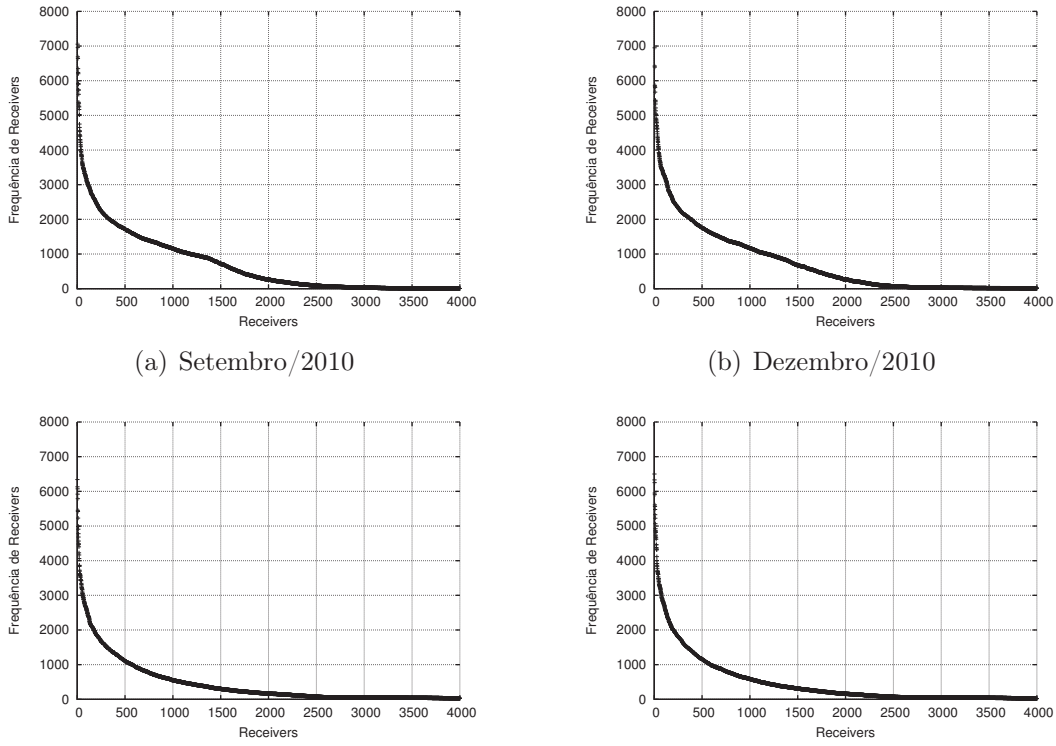
Tal fato, enfatiza a concentração de muitos spams para poucos usuários destinatários. Pode ser observado ainda na Tabela 10 que apesar de ter uma quantidade de destinatários maior como nos meses de 2011, o percentual dos usuários que recebem pelo menos 50% dos spams apresenta um valor muito baixo, não sendo superior a 14% do total de destinatários.

Tabela 10: **Visão geral dos destinatários de spam durante os meses**

Meses	**Total *Recipients***	**# Heavy *Recipients* (recebem 50% spams)**	**% *Recipients* recebem 50% dos spams**
Set/2010	4.243	560	13,19%
Out/2010	4.053	530	13,07%
Nov/2010	4.060	554	13,64%
Dez/2010	5.181	560	10,81%
Jan/2011	5.060	545	10,77%
Fev/2011	5.077	450	8,86%
Mar/2011	5.379	422	8,22%
Abr/2011	5.188	449	8,65%
Mai/2011	5.228	410	7,84%
Jun/2011	5.367	424	7,92%

Fonte: Elaborado pelo autor

Como realizado para os destinatários do *Dataset* de Spam 1, para a análise da popularidade dos destinatários presentes no *Dataset* de Spam 2 foram calculadas as PDFs dos usuários separados por meses. A Figura 5 apresenta a disposição das PDFs dos destinatários de spam dos meses com intervalo de 2 meses entre um e outro, para representar a evolução temporal sem necessitar apresentar as PDFs de cada um dos 10 meses analisados.



(a) Setembro/2010

(b) Dezembro/2010

(c) Março/2011

(d) Junho/2011

Figura 5: PDFs para os destinatários durante os meses selecionados

Pode ser visualizado que as PDFs continuam com o mesmo comportamento analisado no *Dataset* de Spam 1, ou seja, as distribuições seguem uma lei de potência (NEWMAN, 2005), onde poucos destinatários recebem uma quantidade muito grande de spams, enquanto a maioria dos usuários finais são alvos de poucos spammers. Em outras palavras, poucos usuários de spams têm alta popularidade entre os usuários destinatários. Observa-se que a curva da distribuição está sempre bem acentuada e próxima ao eixo y, mostrando que os spams se concentram em poucos usuários, mais precisamente menos de 500 usuários finais.

Portanto, a concentração de muitos spams em um grupo restrito de usuários destinatários como verificado nos 2 primeiros meses (julho e agosto de 2010) referentes ao *Dataset* de Spam 1 foi também identificado no *Dataset* de Spam 2. Pode-se concluir que os spams de fato se concentram em poucos destinatários deste provedor, apresentando uma maior popularidade de certos destinatários que foram considerados foco da recepção de spams. Assim como foi feito na seção anterior, estes usuários destinatários "foco" de spam foram denominados como *Heavy Spam Recipients*.

4.5 Remetentes e Destinatários de E-mail - *Dataset* de E-mail

A análise dos usuários de e-mail foi realizada com intuito de caracterizar a utilização de mensagens eletrônicas pelos usuários de e-mails do provedor. Como o *Dataset* de E-mail possui os e-mails recebidos e/ou enviados pelos usuários do provedor, a caracterização foi realizada na visão dos remetentes de e-mails e dos destinatários de e-mails, pois ambas visões representam o uso de mensagens eletrônicas pelos usuários do provedor de e-mails. É válido ressaltar que esse *Dataset* não possui spams, apenas as mensagens consideradas legítimas. Na sub Seção 4.5.3 é realizada a investigação se os *Heavy Spam Recipients* também são usuários assíduos no envio e recepção de e-mails. Em seguida, é apresentado o *ranking* dos *Heavy Recipients* de spam e e-mail e por fim a identificação desses usuários.

4.5.1 Análise dos Usuários Remetentes de E-mail

A caracterização foi realizada separada por mês durante o período de 12 meses (julho/2010 a junho/2011). Ao contabilizar a quantidade de e-mails enviados verificou-se uma concentração do envio de mensagens eletrônicas em poucos usuários remetentes. Como os dados são anonimizados e o objetivo deste trabalho é caracterizar as contas de usuários pertencentes a esse provedor de e-mails, solicitou-se ao administrador de rede para identificar quais dos domínios presentes no *Dataset* são pertencentes ao provedor. Por exemplo, foi enviada a lista de domínios anonimizados e dentre esses domínios o administrador de redes informou quais são referentes aos 20 domínios pertencentes ao provedor de e-mails em estudo. Com tal informação, foi desenvolvida uma ferramenta que classifica os usuários como pertencentes ou não ao provedor de e-mails a partir da identificação dos domínios. Como resultado é possível visualizar um formulário como apresentado no Quadro 3 que possui valores fictícios apenas para demonstração.

Quadro 3 - Formulário de Identificação dos usuários

Dataset	**Mês/Ano**	**Usuários**	**Pertence ao provedor?**	
			SIM	**NÃO**
Dataset de Email	Julho 2010	remetente-11@dominio19.com.br	X	
		remetente-21@dominio29.com.br	X	
		remetente-21@dominio32.com.br	X	
	Março 2011	remetente-14@dominio42.com.br	X	
		remetente-67@dominio94.com.br	X	
		remetente-80@dominio56.com.br	X	

Fonte: Elaborado pelo autor

Em seguida, foram selecionados os usuários responsáveis por enviar 50% do total de mensagens eletrônicas. Foi verificado que o domínio das contas dos usuários que enviaram 50% do total de e-mails são todos pertencentes ao provedor, ou seja, metade dos e-mails enviados se originam de contas do provedor em estudo. Além disso, foi possível visualizar a concentração do envio de e-mails em poucos usuários, pois dentre as 5.000 contas de e-mail ao selecionar apenas os usuários responsáveis por enviar metade das mensagens eletrônicas obteve-se um número baixo de usuários para cada mês. Na Figura 6 pode-se visualizar essa concentração de envio de e-mails em poucos usuários separados para cada mês.

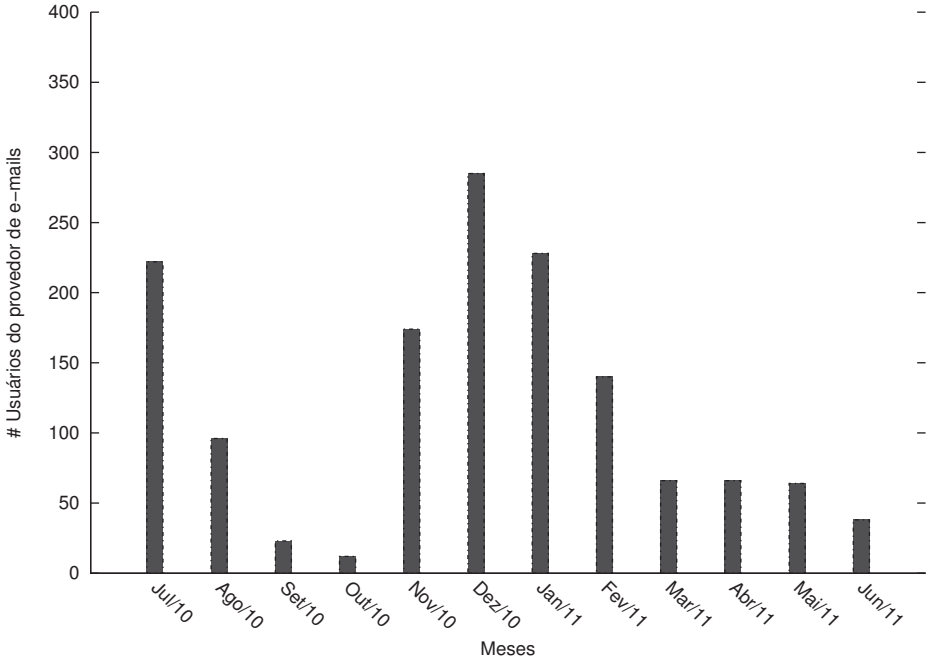


Figura 6: # Usuários do provedor que enviaram 50% dos e-mails

Verifica-se que a quantidade de usuários responsáveis pelo envio de metade dos e-mails sempre se mantém baixa, pois das 5.000 contas de usuários pertencentes ao provedor menos de 400 usuários enviam uma grande quantidade de e-mails em comparação ao total de usuários. Então, foram calculados os percentuais desses usuários entre o total de contas do provedor. Observou-se que durante os 12 meses em média metade dos e-mails são enviados por 8% dos usuários, tal valor mostra a concentração do envio de e-mails em poucos usuários remetentes. Na Tabela 11 são apresentados os percentuais dos usuários responsáveis pelo envio de 50% do total de e-mails enviados do provedor.

Pode-se observar uma variação entre a quantidade de usuários que enviam 50% do total de e-mails. Por exemplo, no mês de dezembro/10 ocorreu uma maior quantidade de usuários que enviaram metade dos e-mails (285 usuários). Tal variação ocorre devido as

Tabela 11: **Visão geral dos remetentes de e-mail durante os 12 meses**

Meses	**Total Remetentes**	**# *Heavy Senders* (enviaram 50% dos e-mails)**	**% Remetentes enviaram 50% dos e-mails**
Jul/10	4.397	222	5,04%
Ago/10	4.155	96	2,13%
Set/10	4.124	23	0,52%
Out/10	4.013	12	0,22%
Nov/10	4.160	174	4,03%
Dez/10	5.120	285	6,12%
Jan/11	5.177	228	4,34%
Fev/11	5.370	140	3,23%
Mar/11	5.189	66	1,02%
Abr/11	5.228	86	2,01%
Mai/11	5.367	94	2,12%
Jun/11	5.223	38	0,71%

Fonte: Elaborado pelo autor

características das contas do usuário do provedor, porém por motivos de privacidade não podem ser divulgadas. Entretanto, ao verificar a contabilização dos registros dos usuários em outros meses, foi observado que um usuário que mandava em média 100 mil e-mails por mês, enviou 60 mil e-mails em dezembro/10. Tal fato, interfere na contabilização dos dados e está diretamente relacionado ao perfil dessa conta o qual não possuímos acesso.

Logo, com os dados apresentados acima pode-se concluir que existe um conjunto de poucos usuários pertencentes ao provedor de e-mails que enviam uma grande quantidade de e-mails, representando os usuários "foco" do envio de e-mail do *Dataset* de Email. Este conjunto de usuários foram nomeados como *Heavy Email Senders*. A seguir, segue a análise dos destinatários de e-mails do provedor.

4.5.2 Análise dos Usuários Destinatários de E-mail

Para os destinatários de e-mails foi realizada a mesma contabilização mensal durante 12 meses. Ao analisar tais usuários, observou-se que assim como nos remetentes apresentados acima, os e-mails que chegam ao provedor se concentram em um conjunto de poucos usuários destinatários. Então realizou-se o mesmo procedimento descrito na subseção anterior, utilizando a ferramenta que classifica os usuários como pertencentes ou não ao provedor de e-mails a partir da identificação dos domínios realizada pelo administrador de rede. A saída dessa ferramenta proporciona um formulário como o apresentado no Quadro 2 citado anteriormente.

Afim de verificar quem são os usuários que recebem mais e-mails que os demais usuários do provedor, foram selecionados os usuários que recebem 50% do total de e-mails

e então utilizou-se a ferramenta citada acima. Na lista de usuários que recebem metade das mensagens eletrônicas do provedor foi verificado que todos essas contas são pertencentes ao provedor de e-mails em estudo. Foi possível visualizar também a concentração de e-mails em poucos destinatários, pois dentre as 5.000 contas de e-mail ao selecionar apenas os usuários que recebem metade das mensagens eletrônicas obteve-se uma quantidade baixa de usuários para cada mês. Na Figura 7 pode-se visualizar essa concentração de e-mails em poucos usuários do provedor separados para cada mês.

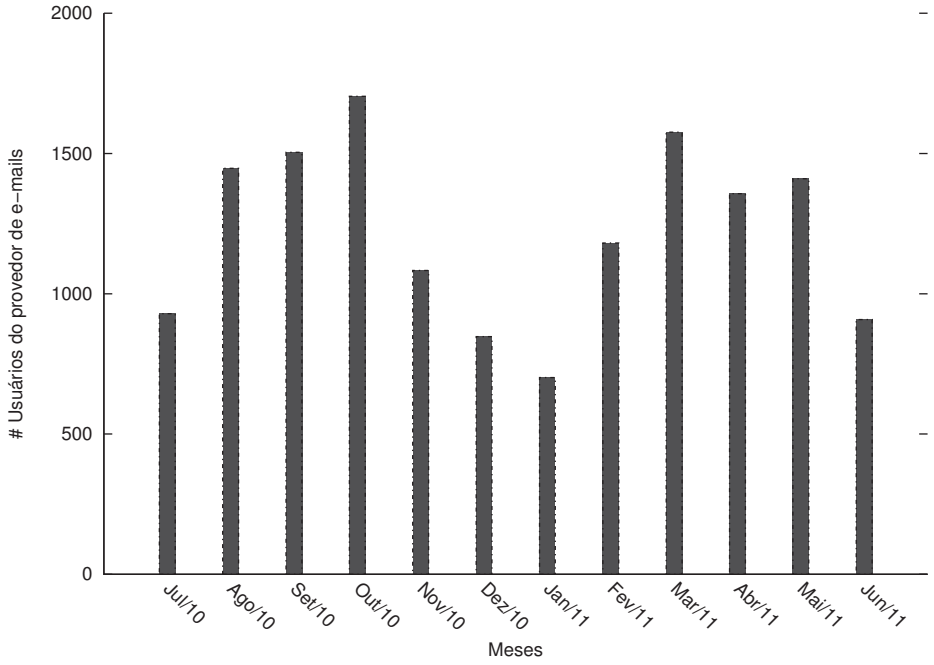


Figura 7: # Usuários do provedor que receberam 50% dos e-mails

Pode ser visto que dentre as 5.000 contas de usuários existente no provedor, a quantidade de usuários que recebem metade dos e-mails do provedor sempre se mantém abaixo de 2 mil usuários, mostrando que menos da metade dos usuários destinatários do provedor recebem 50% das mensagens eletrônicas que chegam ao provedor de e-mails. Para melhor visualização, foram calculados os percentuais desses usuários entre o total de contas do provedor. Na Tabela 12 são apresentados os percentuais dos usuários que recebem 50% do total de e-mails que chegam ao provedor.

Pode ser observado uma variação do percentual de destinatários que recebem 50% das mensagens eletrônicas, por exemplo, em Outubro de 2010 houve uma quantidade muito maior de usuários comparado ao mês de Dezembro de 2010. Essa variação ocorre devido às características do provedor de e-mails em análise e das contas de usuários pertencentes a ele. Entretanto, durante os 12 meses em média metade dos e-mails são recebidos por 26% dos usuários, tal valor mostra a grande quantidade de e-mails recebidos

Tabela 12: **Visão geral dos destinatários de e-mail durante os 12 meses**

Meses	**Total *Destinatários***	**# *Heavy Recipients* (receberam 50% dos e-mails)**	**% Destinatários 50% dos e-mails**
Jul/10	4.420	929	21,01%
Ago/10	4.235	1.447	34,16%
Set/10	4.205	1.504	35,76%
Out/10	4.134	1.704	41,21%
Nov/10	4.223	1.083	25,64%
Dez/10	5.203	847	16,27%
Jan/11	5.195	701	13,49%
Fev/11	5.413	1.181	21,81%
Mar/11	5.225	1.576	30,16%
Abr/11	5.303	1.357	25,58%
Mai/11	5.386	1.410	26,17%
Jun/11	5.298	908	17,13%

Fonte: Elaborado pelo autor

por percentual baixo de usuários destinatários. Com tais dados é possível concluir que para o *Dataset* de E-mails, assim como os *Datasets* de Spam analisados anteriormente, existe um conjunto de usuários "foco" na recepção de mensagens eletrônicas. Este conjunto de usuários foram nomeados como *Heavy Email Recipients*. Este último conjunto de usuários, juntamente com os usuários remetentes "foco" de envio de e-mails (*Heavy Email Senders*) foram classificados como *Heavy Email Users*.

4.5.3 Heavy Spam Recipients X Heavy Email Users

As caracterizações realizadas até o momento permitem concluir que existem usuários "foco" de spam, os quais foram apresentados nas análises dos *Datasets* de Spam 1 e 2. Como visto na subseção anterior existem também usuários "foco" de e-mails legítimos (enviam e/ou recebem grande quantidade de e-mails). Entretanto, seguindo o objetivo deste trabalho, nesta seção busca-se analisar se os usuários destinatários do provedor de e-mails que foram considerados "foco" de spam (*Heavy Spam Recipients*) estão presente entre os usuários classificados como "foco" de e-mails legítimos (*Heavy Email Users*).

A análise da relação desses usuários foi realizada para cada mês no período de julho de 2010 a junho de 2011. Foram construídas as listas dos *Heavy Spam Recipients* e dos *Heavy Email Users* separadas para cada mês. Em seguida, foi desenvolvido um algoritmo que verifica se cada usuário presente na lista de *Heavy Spam Recipients* está presente ou está fora da lista de *Heavy Email Users*. Na Figura 8 é apresentada a relação dos usuários dessas listas para cada um dos 12 meses analisados.

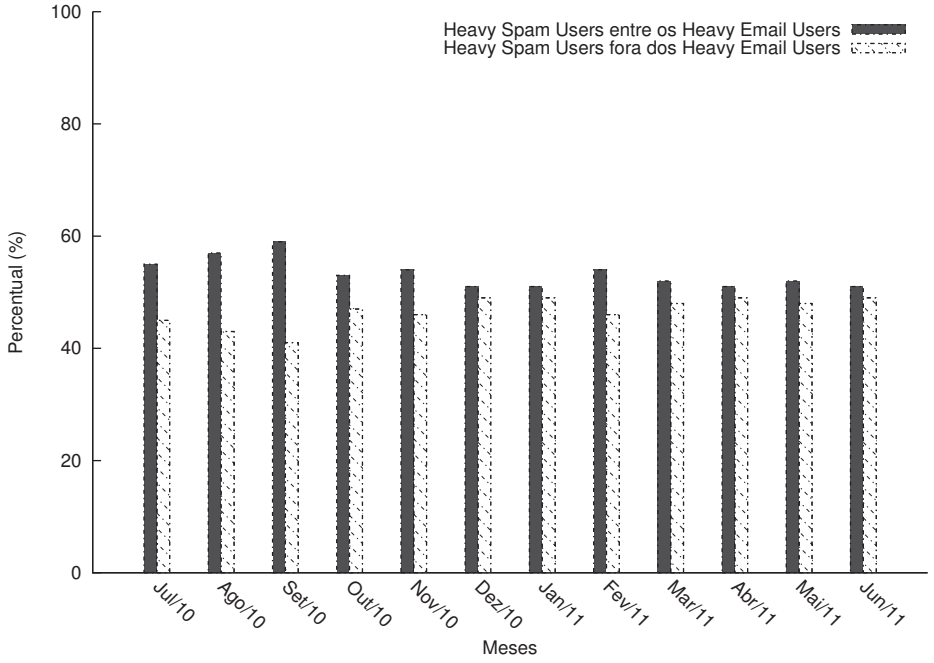


Figura 8: Relação entre *Heavy Spam Recipients* e *Heavy Email Recipients*

As barras preenchidas representam os usuários destinatários "foco" de spam que estão presentes na lista dos usuários destinatários "foco" de e-mail. As barras tracejadas representem os usuários destinatários "foco" de spam que estão fora da lista dos *Heavy Email Recipients*. Por exemplo, no mês de setembro de 2010 do total de usuários de mensagens eletrônicas legítimas, aproximadamente 60% desses usuários também são usuários destinatários "foco" de spam, enquanto aproximadamente 40% representam usuários que não recebem spams e apenas e-mails legítimas. Logo, para todos os meses analisados pode ser visto que as barras preenchidas são sempre maiores que as barras tracejadas, representando que a maioria dos *Heavy Spam Recipients* estão entre os *Heavy Email Users*.

Tal informação tem grande importância, uma vez que um usuário que recebe uma grande quantidade de spams e ao mesmo tempo possui grande fluxo de e-mails pode representar um usuário que prejudique o desempenho dos serviços de e-mail a partir do desperdício de recursos para o tratamento de spams e processamento de mensagens eletrônicas que talvez não seja relevante para o usuário final. Teoricamente, contas de usuários desse tipo podem estar vinculadas, por exemplo, a meios de comunicação ou divulgação representando contas de e-mail mais populares, tal fato pode justificar o enorme fluxo de e-mails e a vulnerabilidade a spams. Porém pode existir contas de usuários que possuem essas características mas estão inutilizadas, apenas congestionando o provedor de e-mails. Para verificar tais suposições, a próxima subseção avalia quais contas de destinatários de spam que permaneceram sempre no topo da lista dos *Heavy Spam Recipients*.

4.5.4 Ranking dos Heavy Spam Recipients

Cada mês analisado possui uma lista dos *Heavy Spam Recipients*. O objetivo desta subseção é identificar os usuários que sempre se mantiveram no topo desta lista durante o período analisado, ou seja, deseja-se ordenar os usuários que receberam maior quantidade de spams durante os 12 meses.

Para isso, foi desenvolvido um *script* que calcula o peso das posições dos usuários em cada uma das 12 listas. Com intuito de enfatizar os peso das primeiras posições, os pesos foram calculados através da soma do inverso das posições dos usuários em cada lista. Por exemplo, um usuário X ficou em segundo lugar na lista de julho/2010 e em quarto lugar na lista de agosto/2010 então o peso desse usuário para esse 2 meses será: $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ e este cálculo foi realizado para os 12 meses. Assim um usuário Y que ficou em quinto lugar em julho/2010 e em vigésimo lugar em agosto/2010 ($\frac{1}{5} + \frac{1}{20} = \frac{1}{4}$) no ranking ficará atrás do usuário X, por ter permanecido em posições maiores nas listas. Então a idéia desse *script* é:

a) Peso da posição = inverso da posição em que o usuários se encontra na lista de cada mês

b) Para cada (Heavy Spam Recipient)$\{\sum (pesoDasPosicoes)\ \}$

Como resultado, possuímos uma única lista contendo os *Heavy Spam Recipients* durante 12 meses ordenados pela quantidade de spams que os usuários "foco" receberam. Lembrando que grande parte destes usuários também são usuários da lista de *Heavy Email Users*. Como visto na subseção 4.5.3 para o provedor de e-mail a identificação de tais usuários e tratamento deles pode trazer muitos benefícios em questão a desempenho e tempo gasto para processamento de mensagens eletrônicas. A próxima seção apresenta uma classificação utilizando esta lista de *Heavy Spam Recipients* dos 12 meses gerada pelo *script* explicado acima, afim de identificar possíveis contas de usuários que, de alguma forma, prejudicam o provedor de correio eletrônico.

4.5.5 Identificação Heavy Spam Recipients

O objetivo desta seção é identificar os usuários da lista gerada a partir do *script* apresentado na subseção 4.5.4, a qual contém os *Heavy Spam Recipients* dos 12 meses ordenados por quantidade de spams que receberam neste período. Vale ressaltar que grande parte dos usuários desta lista também pertencem aos *Heavy Email Users* como analisado na subseção 4.5.3 seja por enviar ou receber muitos e-mails. Logo, a identificação e análise destes usuários pode contribuir para melhorias no provedor de correio eletrônico.

Como os dados são anonimizados, solicitou-se ao administrador de redes uma classificação quanto a utilização das contas de e-mails. Classificou-se como Corporativa, as contas de e-mail vinculadas a meio de comunicação ou divulgação de produtos ou serviços das áreas da organização que utiliza o provedor de e-mail e como conta Pessoal as contas que geralmente é de uso restrito ao proprietário, não estando em meio de divulgação. No Quadro 4 pode ser visualizado o formulário com dados dos 10 primeiros usuários apenas para demonstrar como foi solicitada a classificação.

Quadro 4 - Formulário de classificação dos *Heavy Spam Recipients*

Conta do Usuário	Corporativa?	Pessoal?	Inutilizada?
user-11@dominio19.com.br	X		
user-21@dominio19.com.br		X	
user-21@dominio19.com.br		X	
user-14@dominio19.com.br	X		
user-67@dominio19.com.br	X		
user-34@dominio19.com.br	X		
user-55@dominio19.com.br	X		
user-12@dominio19.com.br	X		
user-98@dominio17.com.br	X		
user-77@dominio19.com.br	X		

Fonte: Elaborado pelo autor

No período dos 12 meses estudados, totalizou-se 702 usuários pertencentes ao grupo dos *Heavy Spam Recipients*, dos quais, foram contabilizados 450 usuários na categoria *Pessoal* e 252 usuários na categoria *Corporativo*. Durante a classificação do formulário enviado o administrador de rede fez observações sobre a existência de contas inutilizadas, pois, pertencem a pessoas já falecidas ou pessoas que já não trabalham mais na organização que utiliza o provedor de e-mails que gerou os dados desta pesquisa. Inclusive foi informado que tais contas serão retiradas do provedor e que deseja-se redefinir as políticas de exclusão de contas.

Para evidenciar que estas contas são inutilizadas, foi analisada no *Dataset* de E-mails como é a utilização dos e-mails legítimos por tais usuários ressaltados pelo administrado de rede. Verificou-se que as contas citadas como inutilizadas pelo administrador apenas recebem e-mails, não havendo e-mails enviados desses usuários no período estudado. Logo, além dessas contas receberem muito mais spams do que os demais usuários, pois estão entre os *Heavy Spam Recipients* elas também recebem muito e-mails, tal fato

contribui para o congestionamento das mensagens eletrônicas e piora do desempenho do provedor de mensagens eletrônicas.

Quanto as contas corporativas e de uso pessoal, pode ser observado no Quadro 4 que apesar da menor quantidade de contas corporativas (252 contas classificadas como *Corporativa* do total de 702 contas), essas estão presentes em maior quantidade no topo da lista de *Heavy Spam Recipients*. Ou seja, recebem muito mais spams que os demais usuários. Como citado anteriormente, as contas de usuários classificadas como *Corporativas* geralmente estão vinculadas a meio de comunicação ou divulgação dos setores da organização que utiliza o provedor de e-mail, tal fato, justifica esta vulnerabilidade quanto aos spams, pois são contas mais populares e expostas em meios públicos de fácil acesso por spammers.

Logo, com os resultados apresentados acima, foi possível concluir que existem contas de usuários com características prejudiciais para o desempenho e bom funcionamento do provedor de e-mails. Além disso, algumas dessas contas não são mais relevantes para os usuários que as possui e outras contas até são totalmente inutilizadas. Através da metodologia apresentada neste trabalho é possível identificar usuários que podem causar problemas ao provedor e portanto devem ser devidamente tratados.

Na seção 2.1 do capítulo 2 apresenta uma das técnicas *antispam* utilizadas que são as *Blacklists* de spams, essas se baseiam na classificação dos usuários que enviam e-mails quanto a confiabilidade, sendo que os usuários não confiáveis são enviados para uma (*blacklists*). Seguindo este raciocínio, esses usuários identificados como prejudiciais ao provedor de e-mails poderiam formar uma *Blacklist* de usuários destinatários do provedor. Essa lista poderia ser baseada na classificação dos usuários a partir da sua utilização de e-mails legítimos e recepção de spams como realizado neste trabalho.

Portanto, usuários destinatários que recebem uma quantidade muito maior de spams e que possuem um fluxo grande de e-mails como encontrado nos usuários destinatários identificados nesta pesquisa, seriam inseridos na *Blacklist* de usuários destinatários do provedor. O comportamento dessa *Blacklist* poderia ser definido de acordo com regras do provedor de e-mails. Ou seja, poderia enviar tais destinatários para uma "quarentena" avisando que eles estão sendo prejudiciais ao provedor, ou se o provedor possuir políticas de controle de e-mails mais rígidas, poderia bloquear as mensagens enviadas para esses destinatários da *Blacklist*, após devidos contatos e comunicados com os donos das contas. Assim as mensagens eletrônicas destinadas para os usuários pertencentes a *Blacklist* de usuários poderiam ser descartadas automaticamente evitando congestionamento do provedor de e-mails para o tratamento desses e-mails inutilizados.

5 CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho foi apresentada e aplicada uma metodologia de caracterização em duas cargas de trabalho que contém os remetentes e destinatários de um provedor de mensagens eletrônicas. A metodologia consiste na caracterização de um conjunto de dados reais coletados na infraestrutura de um provedor de e-mails através de um filtro *antispam* (rede de spams) e registros de mensagens eletrônicas trocadas entre usuários coletadas deste mesmo provedor de e-mails (rede de e-mails), de forma a caracterizar o comportamento e identificar características relevantes nos usuários remetentes e destinatários de spams e e-mails legítimos.

A utilização das métricas popularidade e conectividade, permitiu identificar que os remetentes de spams têm uma conectividade alta, ou seja, os spammers se conectam a vários destinatários. Além disso, foi visto que uma quantidade pequena de spammers têm alta popularidade. Entretanto, a caracterização dos usuários destinatários foi o foco deste trabalho. A análise da popularidade permitiu verificar a existência de um conjunto restrito de usuários destinatários que recebem muito mais spams do que os demais usuários remetentes e destinatários de spams. Tais usuários foram classificados como *Heavy Spam Recipients*. Quanto aos destinatários de e-mails legítimos, também foi observado poucos usuários contento um grande fluxo de e-mails recebidos e/ou enviados, ou seja, usuários com maior popularidade dentre os demais, tais usuários foram classificados como *Heavy Users Email*.

Após essa classificação, foi possível verificar que a maior parte dos usuários presentes no grupo *Heavy Spam Recipients* fazem parte do grupo de usuários com alto fluxo de e-mails (*Heavy Users Email*). Portanto, um destinatário que recebe muitos spams e ao mesmo tempo possui grande fluxo de e-mails legítimos pode representar um usuário que prejudique o desempenho dos serviços de e-mail a partir do desperdício de recursos para o tratamento de spams e processamento de mensagens legítimas que talvez não seja relevante para o usuário final. Para verificar tal suposição, foram identificadas as contas de usuários destinatários de spam que permaneceram sempre no topo da lista dos *Heavy*

Spam Recipients e então foi criado um *ranking* dos usuários que receberam mais spams durante os 12 meses.

Por fim, os usuários dos *ranking* foram classificados e identificados com o auxílio do administrador de redes do provedor de correio eletrônico em estudo. Verificou-se que as contas classificadas como corporativas, que geralmente estão vinculadas a meio de comunicação ou divulgação, estão presentes em maior quantidade no topo da lista de *Heavy Spam Recipients*, ou seja, recebem muito mais spams que os demais usuários. Além disso, verificou-se a existência de contas inutilizadas que só recebem spams e e-mails não sendo mais de uso dos usuários do provedor. A aplicação desta metodologia por um administrador de rede, pode contribuir para um melhor gerenciamento de um provedor de e-mails.

Considera-se como principais contribuições deste trabalho a proposição da metodologia de identificação das contas de usuários com características prejudicais para o bom funcionamento do provedor , bem como a sugestão de criação de uma *Blacklist* de usuários destinatários do provedor, que seriam baseadas na classificação dos usuários a partir da sua utilização de e-mails legítimos e recepção de spams como realizado neste trabalho. A criação de *Blacklist* de spammers, utilizada para o bloqueio de IPs não confiáveis nos servidores é bem conhecida entre as propostas de técnicas *antispam* de várias pesquisas nessa área de tráfego malicioso. Porém, até onde se tem conhecimento, a formação dessas listas focando nos usuários destinatário ainda não havia sido sugerido em trabalhos científicos.

Como trabalho futuro a partir dos resultados encontrados, pretende-se aprofundar a caracterização dos destinatários aplicando outras métricas de redes complexas aos dados estudados. Além disso, analisar o impacto da implementação da *Blacklist* contendo os usuários destinatários do provedor de e-mails que são identificados com a metodologia apresentada neste trabalho. Além de verificar se a *BlackList* de usuários destinatários possibilita alcançar resultados significativos para contribuição na economia de recursos e melhoria do desempenho dos provedores de serviços de e-mail durante o tratamento de mensagens eletrônicas.

REFERÊNCIAS

APACHE SOFTWARE FOUNDATION. **The Apache SpamAssassin Project**. USA: Apache Software Foundation, 2004. Disponível em: <http://spamassassin.apache.org/> Acesso em: 31 jan. 2012.

BARABASI, Laszlo. The origin of bursts and heavy tails in human dynamics. **Nature**, Notre Dame, v. 435, p. 207–211, May 2005.

BENEVENUTO, Fabrício; ALMEIDA, Jussara; SILVA, Altigran. Coleta e análise de grandes bases de dados de redes sociais online. In: JORNADAS DE ATUALIZAÇÃO EM INFORMÁTICA, 2011, Natal. **Anais das Jornadas de Atualização em Informática**. Natal: Sociedade Brasileira de Computação, 2011. p. 11-57.

BERTOLOTTI, Laura; CALZAROSSA, Maria Carla. Workload characterization of mail servers. In: SYMPOSIUM ON PERFORMANCE EVALUATION OF COMPUTER AND TELECOMUNICATION SYSTEMS, 2000, Vancouver. **Proceedings of SPECTS 2000**. Vancouver: Elsevier Science Publishers, 2000. p. 301–307.

BERTOLOTTI, Laura; CALZAROSSA, Maria Carla. Models of mail server workloads. **Performance Evaluation**, Amsterdam, v. 46, p. 65–76, October 2001.

CASTILHO, Luis Henrique *et al*. Caracterização de tráfego smtp na rede de origem. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, n. 28, 2010, Gramado. **Anais do XXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. Gramado: Sociedade Brasileira de Computação, 2010. p. 379–392.

CISCO SYSTEMS. **Cisco 2010 Annual Security Report**. USA: Cisco, January, 2011. Disponível em: < http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf > Acesso em: 31 Jan. 2012.

CLAUSET, Aaron; SHALIZI, Cosma Rohilla; NEWMAN, M. E. J. Power-law distributions in empirical data. **Physics**, Philadelphia, v. 51, n. 4, p. 661–703, Nov. 2009.

COOK, Duncan *et al*. Catching spam before it arrives: Domain specific dynamic blacklists. In: AUSTRALIAN WORKSHOPS ON GRID COMPUTING AND E-RESEARCH. 2006, Darlinghurst. **Proceedings of the 2006 Australian Workshops on Grid Computing and E-Research. Darlingshurst:** Australian Computer Society - ACSW, 2006. p. 193–202.

COOKE, Evan; JAHANIAN, Farnam; MCPHERSON, Danny. The zombie roundup: Understanding, detecting, and disrupting botnets. In: WORKSHOP ON STEPS TO REDUCING UNWANTED TRAFFIC ON THE INTERNET. 2005, Berkeley. **Workshop proceedings and presentation slides. Cambridge:** USENIX Association, 2005. p. 6–6.

EASLEY, David; JON, Kleinberg. **Networks, crowds, and markets:** reasoning about a highly connected world. Cambridge: Cambridge University Press, 2010.

GOMES, Luiz Henrique *et al*. Comparative graph theoretical characterization of networks of spam and legitimate email. In: CONFERENCE ON EMAIL AND ANTI-SPAM, 2, 2005, Stanford. **Proceedings of the Second Conference on Email and Anti-Spam**. Stanford: Stanford University, 2005, p. 9.

GOMES, Luiz Henrique *et al.* Characterizing a spam traffic. In: ACM SIGCOMM CONFERENCE ON INTERNET MEASUREMENT, 4, 2004, New York. **Proceedings of the 4th ACM Sigcomm Conference on Internet Measurement.** New York: ACM, 2004. p. 356–369.

GOMES, Luiz Henrique *et al*. Workload models of spam and legitimate e-mails. **Performance Evaluation**. Amsterdam, v. 64, n. 7-8, p. 690–714, August, 2007.

GOODMAN, Joshua; CORMACK, Gordon V.; HECKERMAN, David. Spam and the ongoing battle for the inbox. **Communications of the ACM**, New York, USA, v. 50, p. 24–33, February 2007.

GUERRA, Pedro H. Calais *et al*. Exploring the spam arms race to characterize spam evolution. In: COLLABORATION ELETRONIC MESSAGING, ANTI-ABUSE AND SPAM CONFERENCE, 7, 2010, Redmond. **Proceedings of the 7th Collaboration Eletronic Messaging, Anti-Abuse and Spam Conference**. Redmond: CEAS, 2010.

HERSHKOP, Shlomo *et al*. Behavior-based modeling and its application to Email analysis. **ACM Transactions on Internet Technology (TOIT)**, v. 6, n. 2, p. 187–221, 2006.

KLUCKHOHN, Clyde. Human behavior and the principle of least effort. **American Anthropologist**, v. 52, n. 2, p. 268–270, 1950.

LAS-CASAS, Pedro Henrique *et al*. Detecção de spammers na rede de origem. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, n. 29, 2011, Campo Grande**. Anais do XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.** Campo Grande: Sociedade Brasileira de Computação, 2011. p. 485–498.

LI, Fulu; HSIEH, Mo-Han. An empirical study of clustering behavior of spammers and group-based anti-spam strategies. In COLLABORATION ELECTRONIC MESSAGING, ANTI-ABUSE AND SPAM CONFERENCE, 3, 2006, Mountain View. **Proceedings of the 3th Collaboration Electronic Messaging, Anti-Abuse and Spam Conference**, Mountain View: CEAS, 2006. p. 1–1.

MESSAGE LABS**. Symantec Intelligence Report**, USA: Message Labs: Symantec Intelligence, July, 2011. Disponível em: < http://br.trendmicro.com/br/products/enterprise/interscan-messaging-security-suite/ > Acesso em: 31 Jan. 2012.

NEWMAN, M. E. J. The structure and function of complex networks. **Society for Industrial and Applied Mathematics Review**, USA, v. 45, n. 2, p. 167–256, 2003.

NEWMAN, M. E. J. Power laws, pareto distributions and zipf's law. **Contemporary Physics**, USA, v. 46, p. 323–351, 2005.

NSS LABS, **Consumer Anti-Malware Products Group Test Report**. USA: NSS Labs, September, 2010. Disponível em: < http://www.nsslabs.com/assets/noregreports/ NSS%20Labs% 20Consumer%20Antimalware%20Group%20Test%20Q3% 202010.pdf> Acesso em: 31 Jan. 2012.

NUCLEUS RESEARCH, **Spam, the repeat offender**. Boston, USA: Nucleus Research, April, 2007. Disponível em: < http://nucleusresearch.com/research/notes-and-reports/spam-the-repeat-offender/ > Acesso em: 31 Jan. 2012

PATHAK, Abhinav; JAFRI, Syed Ali Raza; HU, Y. Charlie. The case for spam-aware high performance mail server architecture. In: CONFERENCE ON DISTRIBUTED COMPUTING SYSTEM, 29, 2009, Washington. **Proceedings of the 29th International Conference on Distributed Computing System**. Washington: IEEE, 2009, p. 155–164.

PAUL, Position Paper *et al*. Understanding and reversing the profit model of spam. In: WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, 4, 2005, Boston. **Proceedings of the 4th Workshop on the Economics of Information Security**: Boston, 2005. p. 11.

PAULSON, Linda Dailey. No quick fix for spam. **Information Technology Professional**, Piscataway, v. 7, n. 3, p. 11–14, May 2005.

POTTERAT, J. J. *et al*. Sexual network structure as an indicator of epidemic phase. **Sexually Transmitted Infections**, v. 78, n. 1, p. 152–158, April 2002.

PU, Calton; WEBB, Steve. Observed trends in spam construction techniques: A case study of spam evolution. In: CONFERENCE ON EMAIL AND ANTI-SPAM, 3, 2006, Mountain View. **Proceedings of the 3th Conference on Email and Anti-spam**: Mountain View, 2006. p.104.

RAMACHANDRAN, Anirudh; FEAMSTER, Nick. Understanding the network-level behavior of spammers. **Computer Communication Review**, New York, v. 36, p. 291–302, August 2006.

RAMACHANDRAN, Anirudh; FEAMSTER, Nick; VEMPALA, Santosh. Filtering spam with behavioral blacklisting. In: CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 14, 2007, New York. **Proceedings of the 14th Conference on Computer and Communications Security**: ACM. 2007. p. 342–351.

SAHAMI, Mehran *et al*. A bayesian approach to filtering junk e-mail. In: LEARNING FOR TEXT CATEGORIZATION: PAPERS FROM THE WORKSHOP, 1998, Madison. **Proceedings of the American Association for Artificial Intelligence Workshop:** Madison, 1998, v. 62, p. 98–105.

SERJANTOV, Andrei; CLAYTON, Richard. Modelling incentives for email blocking strategies. In: WORKSHOP ON THE ECONOMICS OF INFORMATIONS SECURITY, 4, 2005, United Kingdom. **Proceedings of the 4th Workshop on the Economics of Information Security**, University of Cambridge, 2005, p. 2–3.

SHANNON, E.C. A mathematical theory of communication. **Mobile Computer and Communication Review**, New York, v. 5, p. 3–55, January 2001.

SYMANTEC**. State of Spam e Phishing Monthly Report**. USA: Symantec, October, 2011. Disponível em: < http://www.symantec.com/content/en/us/enterprise/other_ resources/b-intelligence_report_10-2011.en-us.pdf> Acesso em 31 Jan. 2012.

TWINING, Richard Daniel *et al*. Email prioritization: reducing delays on legitimate mail caused by junk mail. In: USENIX ANNUAL TECHNICAL CONFERENCE, 4, 2004, Berkeley. **Proceedings of the 4th Usenix Annual Technical Conference**: USENIX Association, 2004, p. 4–4.

TREND MICRO. **InterScan Messaging Security Suite**. USA: Trend Micro, April 2007. Disponível em: <http://br.trendmicro.com/br/products/enterprise/interscan-messaging-security-suite/ > Acesso em 31 Jan. 2012.

WATTS, D J; STROGATZ, S H. Collective dynamics of "small-world" networks. **Nature**, v. 393, n. 6684, p. 440–442, 1998.

WEINSTEIN, Lauren. Spam wars. **Communications of the ACM**, New York, v. 46, p. 136, August 2003.