Caracterização e Análise de Redes de Remetentes e Destinatários de SPAMs

Thaína Amélia de Oliveira Alves[1], **Humberto T. Marques-Neto**[1]

[1] Departamento de Ciência da Computação
Pontifícia Universidade Católica de Minas Gerais (PUC Minas)
30.535-901 - Belo Horizonte - Brasil

thaina.alves@sga.pucminas.br, humberto@pucminas.br

Abstract. *The interaction between senders and receivers of electronic messages (emails) can be studied as a complex network of information exchange that represents the process of communication between people involved. This article characterizes the networks formed from this exchange of emails recorded in a log generated by the real filter spam from an email provider. The results show that typical metrics of complex networks, such as popularity and connectivity can be used to assist the identification of malicious users (spammers). We observed that few spammers have high popularity and high connectivity in the network. This characterizes users that can affect the performance of electronic mail service, disseminating large quantities of unwanted messages that are probably to be processed and discarded at their destination.*

Resumo. *A interação entre remetentes e destinatários de mensagens eletrônicas (e-mails) pode ser estudada como uma rede complexa de troca de informações que representa o processo de comunicação entre as pessoas envolvidas. Este artigo caracteriza as redes formadas a partir dessa troca de e-mails registrada em um log real gerado pelo filtro de spam de um provedor de correio eletrônico. Os resultados mostram que métricas típicas de redes complexas, tais como popularidade e conectividade, podem ser utilizadas para auxiliar a identificação de usuários maliciosos (spammers). Observou-se que poucos spammers possuem alta popularidade e alta conectividade na rede, caracterizando usuários que podem afetar o desempenho do serviço de correio eletrônico ao disseminarem grande quantidade de mensagens indesejadas que, provavelmente, serão processadas e descartadas no seu destino.*

1. Introdução

Cada vez mais a Web vem se transformando em um meio para a disseminação de conteúdo entre pessoas relacionadas direta ou indiretamente. Juntamente com esse crescimento, percebe-se também um aumento no volume de e-mails indesejados e não solicitados (spams). Esforços dedicados ao bloqueio de spams também ocorrem de maneira significativa. Apesar desses esforços, e-mails indesejados ainda representam cerca de 90% de todos e-mails trafegados na Internet [Symantec 2011].

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 [IronPort Email and Web Security 2011]. No relatório do [Message Labs 2011], pode ser

visto que em fevereiro de 2011 a taxa de spams por e-mail trafegado aumentou 2,7% comparado ao mês anterior (1 em cada 1.23 mensagens de e-mail). Apesar da existência de mecanismos dedicados ao bloqueio de spam, ainda nota-se a chegada de muitas mensagens indesejadas na caixa de entrada dos destinatários.

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 indesejados. Entretanto, a filtragem realizada por esses mecanismos pode ser ineficiente devido a falta de conhecimento do comportamento dinâmico de spammers nas redes de e-mail. Tal fato, é evidenciado no relatório da [Nucleus Research 2007], que mostra que o spam não filtrado, ou seja, que precisa ser filtrado pelo próprio usuário, acarreta uma queda de produtividade em cerca de 1,2% por empregado ao ano, causando prejuízos para as empresas. Essa grande quantidade de spams que circulam na Internet acaba afetando o desempenho dos provedores de e-mail e, consequentemente, causa desperdício de recursos para o tratamento do tráfego de spam na rede [Dan Twining 2004]. Prejuízos desse tipo poderiam ser minimizados com a análise dos spammers para sua efetiva identificação.

A troca de informações entre pessoas através do uso de um serviço de correio eletrônico tem estrutura semelhante a uma rede complexa, que é definida em [Easley and Jon 2009] como uma rede que possui uma topologia com caracaterísticas específicas, tais como, alto coeficiente de agrupamento, caudas pesadas em distribuições de probabilidade e reciprocidade. Sendo assim, sugere-se que a rede de remetentes e destinatários de spams desta pesquisa seja estudada como uma rede complexa, a partir da análise de características como reciprocidade, conectividade e popularidade dos nós da rede. A reciprocidade será discutida na Seção 2, as duas últimas características serão analisadas mais especificamente na Seção 4.

O aumento das redes formadas por usuários de e-mails e do conteúdo malicioso existente nelas, motiva a identificação de possíveis efeitos negativos na atuação dos correios eletrônicos. Através de algumas métricas de redes complexas tais como, popularidade e conectividade, é possível identificar características desse processo de troca de informações [Easley and Jon 2009]. A popularidade é um fenômeno caracterizado por desequilíbrios extremos, no contexto dessa pesquisa seria poucos destinatários recebendo muitos spams enquanto a maioria dos destinatários recebendo poucos spams. Já a conectividade representa se os remetentes da rede ao enviarem spams atingem os destinatários de forma regular, possuindo conexão com vários destinatários. Ao analisar tais métricas, pode ser possível identificar focos de spams.

Este artigo caracteriza, através do uso de métricas de redes complexas, uma rede de troca de informações formada pelos remetentes e destinatários de spams presentes em um log real gerado pelo filtro antispam de um provedor de e-mails. Tal análise busca identificar possíveis usuários focos de recepção de tráfego malicioso, pois eles podem causar problemas de desempenho dos serviços de e-mail a partir do desperdício de recursos para o tratamento de mensagens que, provavelmente, serão descartadas no seu destino.

O restante deste trabalho está organizado em 5 seções. Os trabalhos relacionados são discutidos na Seção 2. Na Seção 3 é descrita a metodologia de caracterização. A Seção 4 apresenta e analisa os resultados relevantes para este trabalho e na Seção 5 é apresentada a conclusão e possíveis trabalhos futuros.

2. Trabalhos Relacionados

Diversas pesquisas na área de caracterização de tráfego malicioso buscam identificar as estratégias e comportamento dos spammers. O trabalho de [Ramachandran and Feamster 2006] analisa as estratégias dos spammers no nível de infraestrutura da rede. Os autores apresentam características da origem das mensagens e concluem que o envio de spams acontece em faixas restritas de endereços de IPs. Em outra pesquisa nesta mesma corrente realizada por [Li and Hsieh 2006], observou-se o surgimento de grandes grupos de IPs que enviam spams referenciando repetidas URLs contidas no conteúdo das mensagems de spam.

Na busca por diferenciar comportamentos maliciosos de comportamentos legítimos, a pesquisa de [Gomes et al. 2004] caracteriza e analisa uma carga de trabalho com base em alguns critérios, tais como, tamanho das mensagens e processo de chegada. Foi possível identificar que o comportamento malicioso (spam) e o comportamento legítimo se diferenciam em muitos dos aspectos. Em [Gomes et al. 2009] foi observado 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.

O trabalho de [Pu and Webb 2006] faz uma análise de mensagens enviadas, avaliando as técnicas que os spammers utilizam para construir as mensagens. Os autores mostraram que algumas técnicas deixam de ser usadas devido a fatores como correção na segurança de programas. Por outro lado, outras estratégias persistem por mais tempo. Levando em conta este comportamento dinâmico dos spammers, o trabalho de [Gomes et al. 2005] analisa quantitativamente um tráfego de e-mail verificando várias características, entre elas, a entropia dos fluxos de entrada e de saída de cada nó da rede, como proposto por Shannon [C.E Shannon 1948]. Essa pesquisa mostrou que o tráfego legítimo apresenta menor entropia do que o tráfego oportunista gerado pelo envio de spams.

Ainda em questão a natureza dinâmica dos spammers a pesquisa de [Guerra et al. 2010] avalia filtros antispam para a análise de tendências de spam, pois, eles são os agentes que podem forçar os spammers a mudar suas táticas. Para esta pesquisa foram utilizados filtros antigos e recentes do Open Source filter Spam Assassin [Project 2010] para comparar spams dos últimos 12 anos. Os resultados mostram que técnicas de spammers mudam a medida que filtros começam a detectá-las.

As pesquisas citadas acima apontam um grande dinamismo do comportamento dos spammers, o que é um fator agravante para os servidores de e-mails que gastam cada vez mais recursos no combate às mensagens não legítimas [Pathak et al. 2009]. Quanto aos prejuízos que os spams podem causar, o estudo de [Dan Twining 2004] verifica que spammers são prejudiciais para o desempenho de servidores de e-mail, uma vez que o tratamento de spams podem congestionar a chegada de e-mails válidos para os usuários finais.

A pesquisa de [Dan Twining 2004] se relaciona ao presente artigo, porém aqui busca-se identificar e analisar os usuários que podem prejudicar o desempenho dos provedores de e-mail. Além disso, este trabalho também se baseia em métricas de redes complexas, como a popularidade e a conectividade, afim de verificar a existência de usuá-

rios focos de spam da rede de informações formada, onde os remetentes e destinatários representam os nós e a relação entre eles determinada pelo envio de e-mails são os *links*.

Segundo [Easley and Jon 2009], a popularidade de uma rede complexa é representa por uma lei de potência [M. E. J. Newman 2006]. Quando uma função decresce a medida que um valor K é elevado, tal função segue uma lei de potência. Em outros termos, poucos usuários possuem alta frequência de utilização da rede, e quando essa frequência de uso diminui a quantidade de usuários aumenta, mostrando que "poucos usuários utilizam muitos recursos da rede". Além da popularidade, a conectividade entre os remetentes e destinatários também será analisada para os spammers da rede.

3. Metodologia de Caracterização

Esta Seção apresenta a metodologia de caracterização que delineia o processo de análise do comportamento dos usuários de e-mail, quantificando e qualificando os registros do log gerado pelo filtro de spam de um provedor de serviços de correio eletrônico. Entender as características do comportamento dos remetentes e destinatários de spams é uma tarefa que pode contribuir para o desenvolvimento e evolução de técnicas para detectar spammers, possibilitando assim estabelecer uma melhoria nos serviços de e-mails.

O conjunto de dados reais utilizado neste estudo foi coletado na infraestrutura de um provedor de e-mails 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]. O log 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 deste log 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, classificação do spam, bem como outros dados do cabeçalho da mensagem. É válido ressaltar que o log está anonimizado não sendo possível identificar tais usuários (remetentes ou destinatários) na sociedade.

3.1. Visão Geral da Carga de Trabalho

Inicialmente foi realizada uma contabilização geral do conteúdo do log. 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. Pode ser observado de acordo com a quantidade de remetentes e domínios, a proporção de 1 domínio para cada 10 remetentes distintos, o que mostra 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. Novamente podemos observar uma grande concentração de usuários receptores de spams para um mesmo domínio. Além disso, tendo em vista que tais usuários em média receberam

aproximadamente 1.000 spams no período de 2 meses da coleta do log, foi possível verificar a existência de usuários focos, ou seja, usuários que recebem uma grande quantidade de spams em comparação a média geral. Particulamente, 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 de e-mail. Uma visão geral da distribuição dos remetentes e destinatários de spam são apresentados na Tabela 1. 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.

Tabela 1. Contabilização dos remetentes e destinatários distintos de Spams

Log	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
				Total de E-mails	5.762.534

Para modelar a rede complexa 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 *Receivers*. Os remetentes foram identificados através de seus IPs devido ao seu comportamento dinâmico (vide Seção 2). Além desses campos utilizados para identificação da rede complexa, o campo classificação do spam também é relevante, pois, é responsável por informar a gravidade do spam, de acordo com configurações pré-definidas pelo filtro antispam da *Trend Micro*. A Figura 1 apresenta a estrutura do campo classificação presente nos registros do log analisado e em seguida, apresenta-se a definição de cada campo desta classificação:

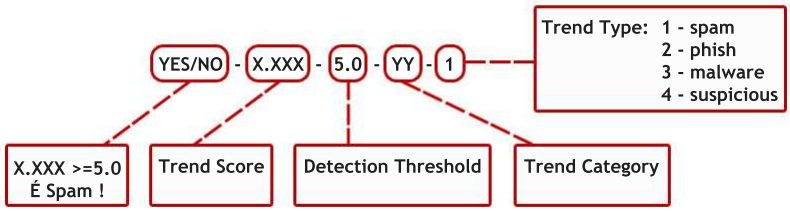


Figura 1. Campo Classificação do Spam

- O primeiro campo informa se o e-mail foi considerado spam (*Yes* ou *No*).
- *Trend Score*: representa a "pontuação" do spam utilizando regras pré-definidas.
- *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 log foi utilizada a configuração com o nível médio.
- *Trend Category*: define qual categoria o spam pertence; não é utilizado para esta coleta, ou seja, todos spams são de uma mesma categoria.
- *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*.

Após a contabilização geral, foram realizadas análises quantitativas nos dados da rede formada pelos usuários presentes no log. As distribuições de frequência acumulada e probabilidade dos usuários (remetentes e destinatários) foram calculadas para a análise da popularidade e da conectividade dos spams na rede, afim de identificar os usuários focos de spam. Na Seção 4 serão apresentadas essas análises.

3.2. Seleção e Classificação dos dados da Carga de Trabalho

Para obter uma melhor visualização dos dados e identificação das características dos usuários, a rede de remetentes e destinatários de spams foi analisada separada por semanas. Para isso, foram selecionadas 4 semanas entre julho e agosto 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. A análise dessas semanas foram realizadas considerando os dois pontos de vista:

- *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 presentes na rede.
- *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 presentes na rede.

Durante a organização dos registros 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 como citado na Subseção anterior. 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.

4. Resultados

Esta Seção apresenta e discute os principais resultados encontrados na caracterização da rede de remetentes e destinatários de spams em estudo. Inicialmente apresentamos a análise das métricas de redes complexas relevantes para o artigo e, em seguida, é apresentada uma classificação realizada a partir dos usuários de trocas de e-mail (remetentes e destinatários). Então, foi realizada as análises dos dados separadamente para cada tipo de classificação dos usuários.

4.1. Seleção das métricas da teoria de Redes Complexas

A partir da rede formada pelos usuários de troca de e-mails, foi possível analisar a popularidade e a conectividade dos usuários, porém, a conectividade foi analisada apenas para os remetentes, pois, como vimos na Seção 2 os spams não possuem reciprocidade.

Através dessas métricas podemos identificar a existência dos usuários que mais enviam e que mais recebem spams na rede, ou seja, usuários mais "populares" na rede. Estes usuários podem prejudicar o desempenho do serviço de e-mails ao disseminarem grande quantidade de spams.

Como apresentado na Seção 2 a popularidade é representada por uma lei de potência [M. E. J. Newman 2006], ou seja, poucos usuários possuem alta frequência de utilização da rede, e quando essa frequência de uso diminui a quantidade de usuários aumenta. Assim como a popularidade, a conectividade dos usuários na rede também é uma importante métrica, pois, através dela, pode-se avaliar se a disseminação de conteúdo malicioso na rede ocorre a partir dos usuários com alta conectividade.

4.2. Análise da rede de Remetentes e Destinatários de Spams

Com o intuito de entender a propagação dos spams na rede formada a partir dos usuários de troca de e-mails, a análise dos usuários da rede foi realizada considerando os dois pontos de vista (Remetentes de spams e Destinatários de spams) citados na Seção 3.2. Nas Subseções a seguir são apresentadas para cada grupo definido acima, as análises dos usuários da rede e das métricas de redes complexas selecionadas.

4.2.1. Análise dos IPs Remetentes de Spam

A análise dos IPs Remetentes foi realizada para cada uma das 4 semanas selecionadas, (vide Seção 3.2). Contabilizando os spams enviados de cada semana e relacionando-os aos IPs Remetentes responsáveis, na semana 1 cerca de 4% dos IPs Remetentes foram responsáveis pelo envio de 50% dos spams da rede, sendo 5% na semana 2 e 6% na semana 3 e 4, apresentando uma média de 5% durante as 4 semanas.

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 na Seção 2 desse artigo, 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. Tal ocorrência é apresentada na Tabela 2 a seguir.

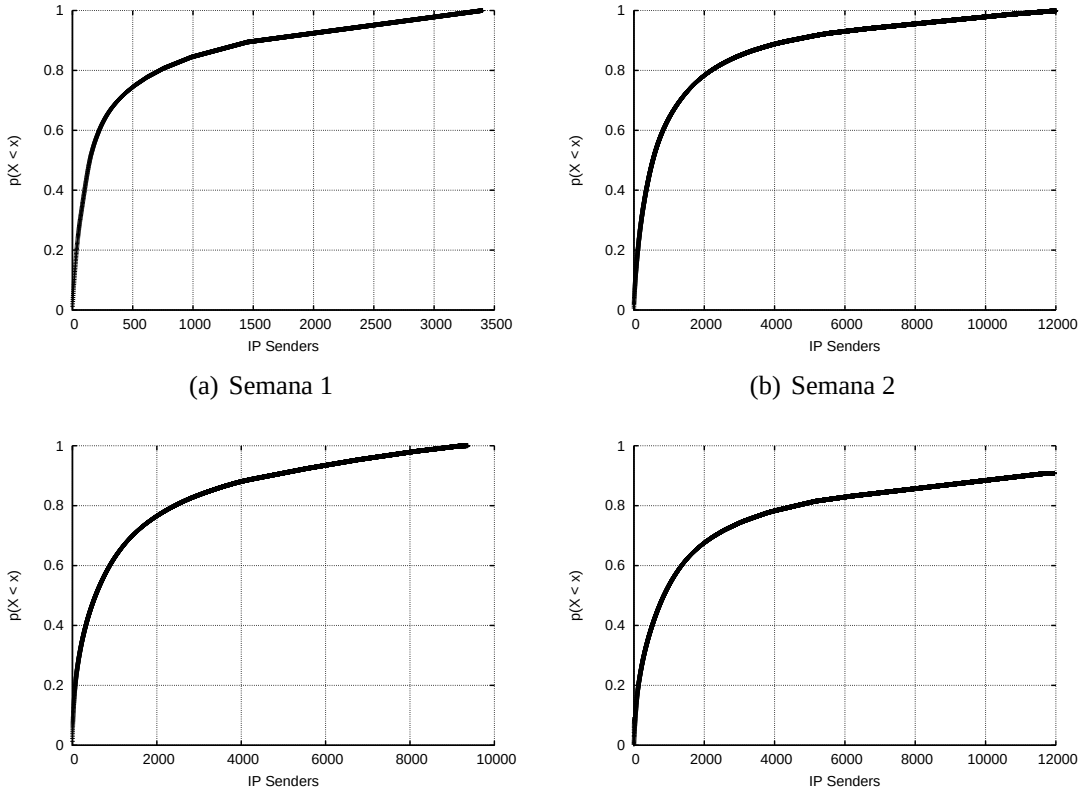
Tabela 2. Modificação dos spammers de um mesmo IP durante as semanas.

Semana	IPs	Remetentes	# Spams Enviados
1	63.201.115.98	rmt23987@dmn13.com.br	20
2	63.201.115.98	rmt134298@dmn13.com.br	193
3	63.201.115.98	rmt237893@dmn13.com.br	381
4	63.201.115.98	rmt365278@dmn13.com.br	386

Para analisar a conectividade dos spammers da rede foram contabilizados os e-mails trocados entre os usuários da rede. 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, verificamos que dentre os 6 milhões de spams bloqueados pelo filtro, estes se espalham regularmente

entre os destinatários da rede, onde em média os usuários destinatários recebem cerca de 1.700 e-mails. Isso mostra que os *senders* atingem constantemente todos os destinatários da rede. 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 focos.

Para analisar a popularidade dos nós (usuários) dessa rede foram calculadas as CDFs [1] e as PDFs[2] dos usuários separados por semanas. Na Figura 2 é possível visualizar a disposição da curva CDF dos IPs Remetentes de spams durante as 4 semanas. Pode ser visto nas CDFs que a curva da distribuição está sempre bem acentuada e próxima ao eixo y, mostrando que os IPs Remetentes de spams se concentram em poucos usuários, mais precisamente menos que 2 mil spammers. Com isso, observa-se que o envio de spam de fato se concentra em poucos IPs Remetentes, mostrando uma maior popularidade de certos spammers que podem ser considerados focos da disseminação de spams na rede.



(a) Semana 1 (b) Semana 2

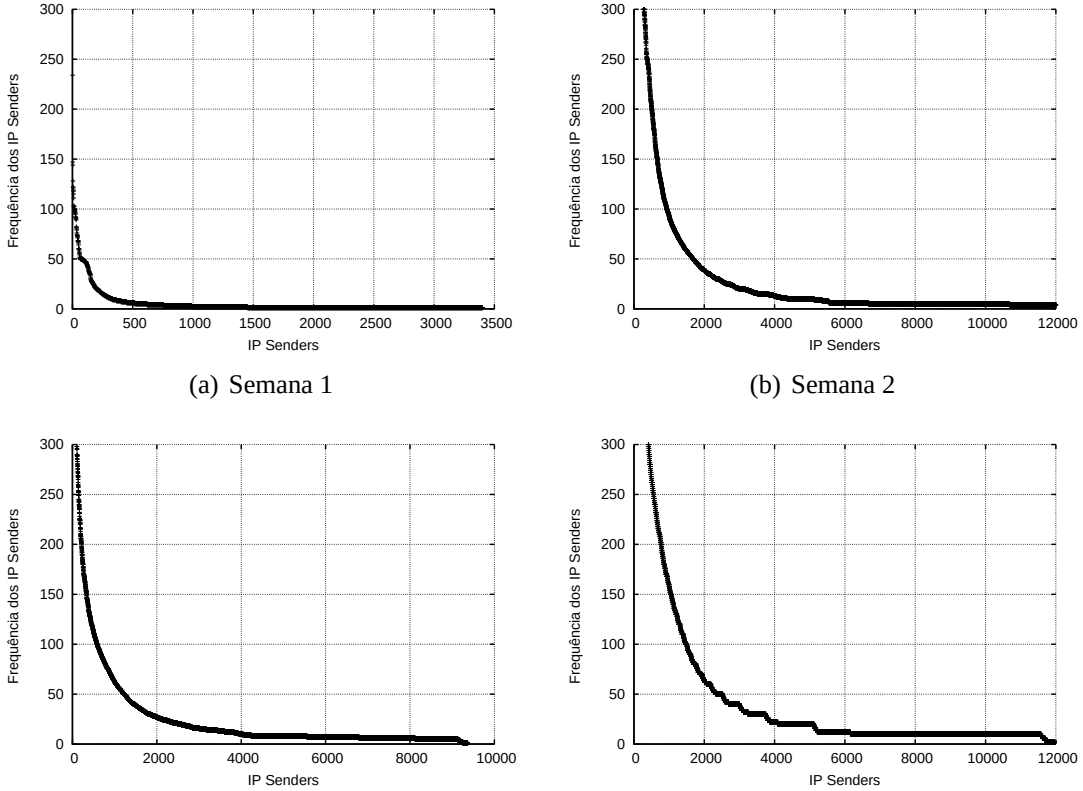
(c) Semana 3 (d) Semana 4

Figura 2. CDFs para os *IPs Remetentes* durante as 4 semanas

Além das CDFs, que apresenta a distribuição de frequência acumulada dos remetentes na rede, podemos também análisar as PDFs da rede formada. A Figura 3 apresenta a disposição das curvas das PDFs dos IPs Remetentes de spam. Pode ser visualizado nas PDFs um comportamento típico de uma lei de potência [M. E. J. Newman 2006], pois implica que poucos remetentes enviam spam para uma grande quantidade de usuários finais,

[1] *Cumulative Distribution Frequency (CDF)*
[2] *Probability Distribution Frequency (PDF)*

enquanto a maioria dos spammers envia mensagens maliciosas para poucos destinatários. Em outras palavras, poucos nós da rede de remetentes de spam têm alta popularidade entre os usuários.



(a) Semana 1 (b) Semana 2

(c) Semana 3 (d) Semana 4

Figura 3. PDFs para os *IPs Remetentes* durante as 4 semanas

Para melhor visualizar tal fato, foram selecionados dentre os IPs Remetentes aqueles que enviaram 50% dos spams da rede para cada semana selecionada. Estes usuários foram denominados como *Heavy Senders*. É possível ver na Tabela 3 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 focos de envio de spams.

Tabela 3. Visão geral dos remetentes de spam durante as semanas

Semana	**# IPs Remententes**	**# 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%

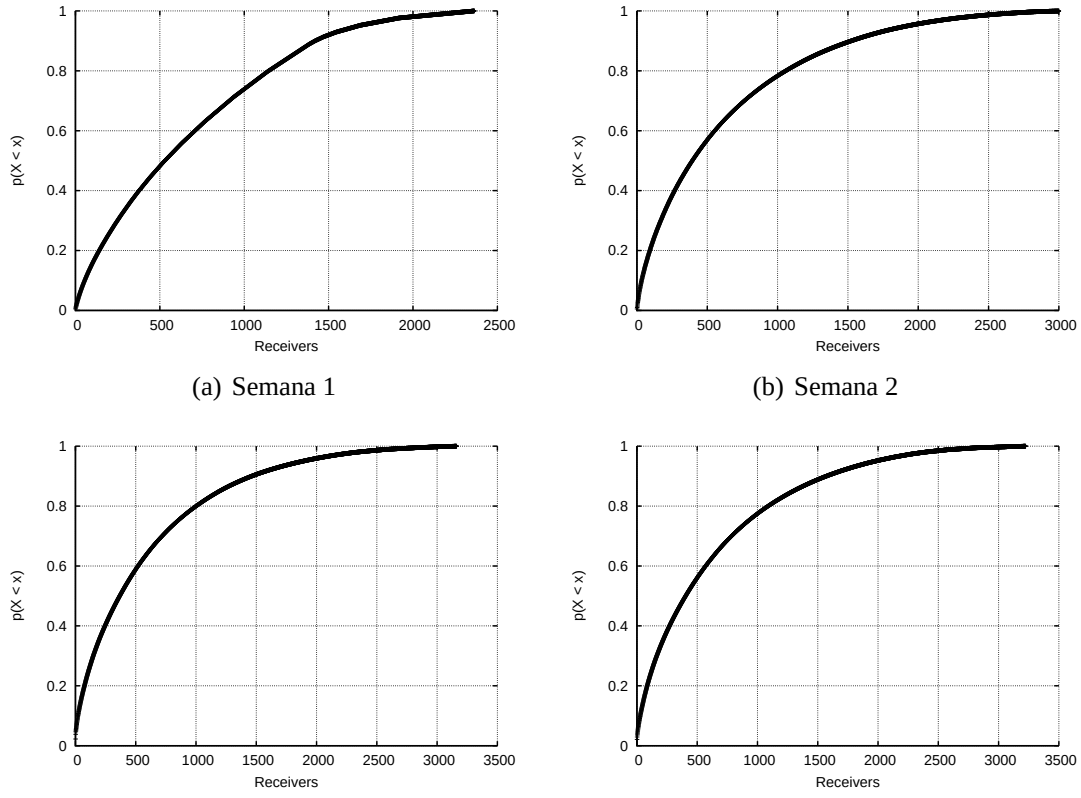
A descoberta de dados desse tipo, como a concentração de envio de spam em poucos remetentes é útil para possíveis melhorias na rede de correio eletrônico, pois, ao tratar tais usuários focos de spam, pode-se evitar o desperdício de recursos para combater os spammers e consequentemente melhorar o desempenho de serviços de e-mail. Isso pode acontecer também com destinatários focos de spams, que são analisados a seguir.

4.2.2. Análise dos Destinatários de Spam

A análise dos destinatários de spams também foi realizada para cada uma das 4 semanas selecionadas. Ao contabilizar a quantidade de spams enviados para um determinado usuários final, encontrou-se focos 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.

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.

A popularidade de certos destinatários de spam, assim como os remententes, também se concentram em poucos usuários. A Figura 4 apresenta as curvas CDF dos destinatários de spam em cada semana destacada para o estudo. Observa-se que essas curvas 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 finais de spams. Tal fato pode ser observado também na Figura 5 que apresenta as curvas PDFs dos destinatários de spams durante as 4 semanas selecionadas.

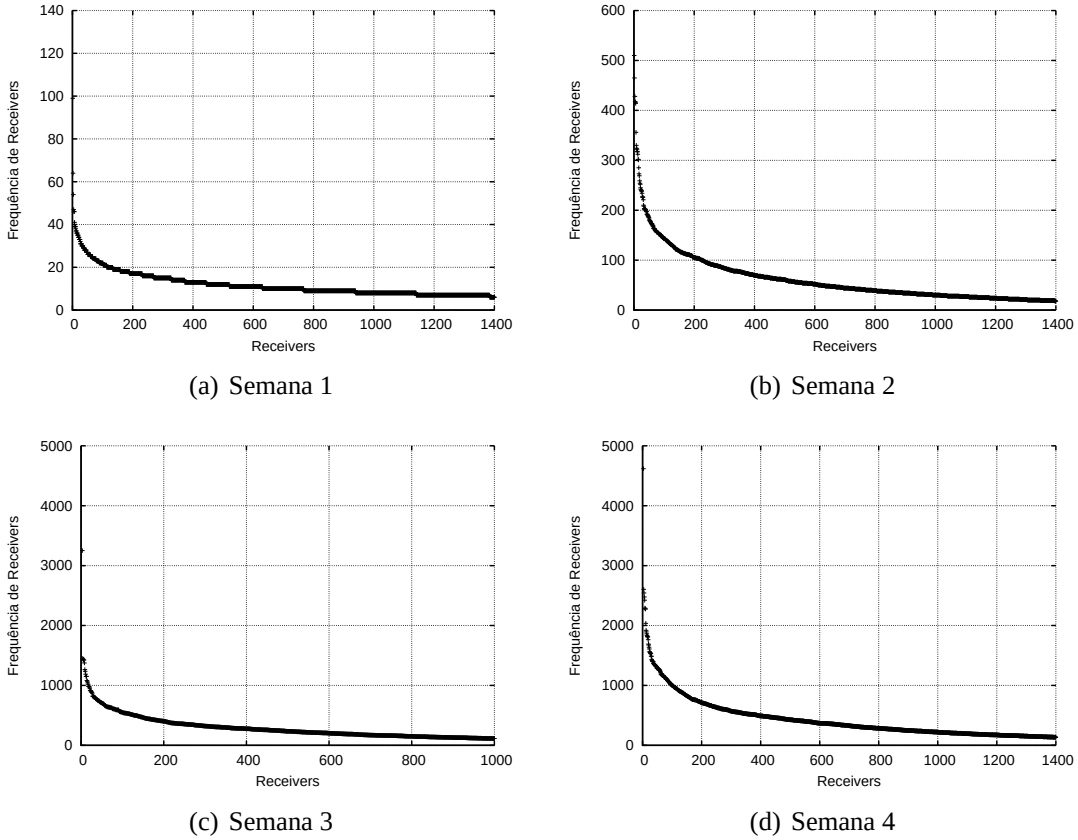


(a) Semana 1 (b) Semana 2

(c) Semana 3 (d) Semana 4

Figura 4. CDFs para os destinatários durante as 4 semanas

Assim como nos remetentes analisados na Subseção anterior, as PDFs dos destinatários de spam também apresentam um comportamento típico de uma lei de potência. Isto



(a) Semana 1 (b) Semana 2

(c) Semana 3 (d) Semana 4

Figura 5. PDFs para os destinatários durante as 4 semanas

aponta que poucos usuários receberem muito spam, enquanto a maioria dos usuários destinatários recebem menor quantidade de spams. Pode-se concluir também que poucos nós da rede de destinatários de spam têm alta popularidade entre os IPs Remetentes. Na Tabela 4 tal fato pode ser melhor visualizado. 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. Assim como foi feito para os remetentes, estes usuários foram denominados como *Heavy Receivers*.

Tabela 4. Visão geral dos Destinatários de Spam durante as semanas

Semana	**Total *Receivers***	**Quantidade Heavy *Receivers* (recebem 50% spams)**	**% *Receivers* que 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%

Analisando pela visão do administrador de redes, 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 na pesquisa de [Dan Twining 2004].

4.3. Movimentação dos Spams na rede de Remetentes e Destinatários

Como visto na Seção 2, as pesquisas apontam um grande dinamismo do comportamento dos spammers. 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 na rede. A cada semana os remetentes de spam são alterados continuando poucos com o mesmo IP. Na Tabela 5 é apresentada a movimentação de entrada e saída de IPs durante este período de 4 semanas.

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

Observa-se que a quantidade de IPs novos ou que saem 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 e 868 novos IPs entraram. Tais dados mostram a constante alteração dos remetentes ao enviarem spams para seus destinatários.

4.4. Classificação dos Spams da rede de Remetentes e Destinatários

Outro fator interessante da análise dos spammers neste estudo é a classificação do spam que foi enviado. Esta classificação, como visto na Seção 3.1, é realizada pelo filtro antispam utilizado pelo provedor de e-mails no qual o log foi coletado. Através desse campo de classificação é possível identificar a gravidade de cada spam recebido pelo provedor. Como citado anteriormente na Seção 3.2, foram armazenados os valores máximos, mínimos e as médias dos *Trend Scores* dos e-mails da rede de remetentes e destinatários em estudo. 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 6 são apresentados os valores médios dos *Trend Scores* contabilizados de forma geral para a rede. Ela mostra também a média dos *Trend Scores* para os *Heavy* spams e a média dos *Trend Scores* para "*Light*" spams, esse último grupo representa os demais usuários da rede que não foram considerados focos de spam.

Tabela 6. *Trend Score* IPs *Senders*

Semana	Média Geral		Média Heavy		Média Light	
	Senders	***Receivers***	***Senders***	***Receivers***	***Senders***	***Receivers***
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

Pode ser visto que para os *Heavy* spams a média do *Trend Score* é sempre mais alta, como, por exemplo, a semana 4, em que a média geral do *Trend Score* dos *Receivers* é 14,0 e a média dos *Heavy* e *Light receivers* são respectivamente 47,6 e 9,18. Tais dados mostram a maior gravidade dos spams recebidos pelos *Heavy receivers* e enviados pelo *Heavy senders*.

Este é mais um fator importante entre as características da rede de remetentes e destinatários deste artigo, 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 os usuários que enviam ou recebem spams considerados mais graves, o desempenho de filtros antispam e serviços de e-mail serão diretamente beneficiados.

5. Conclusão

Neste trabalho foi apresentada e aplicada uma metodologia de caracterização da rede de remetentes e destinatários de spams de um provedor de mensagens eletrônicas. A metodologia consiste na análise de um conjunto de dados reais coletados na infraestrutura de um provedor de e-mails através de um filtro antispam, de forma a identificar características relevantes no comportamento de spammers e destinatários de spams.

A análise das métricas de redes complexas, popularidade e conectividade, permitiu identificar que alguns grupos de remetentes e destinatários de spams possuem alta popularidade na rede. Além disso, foi visto que os remetentes da rede de spam tem uma conectividade alta, ou seja, os spammers se conectam a vários destinatários. Quanto às características dos spams enviados, analisando o campo de classificação de spams existente nos registros, percebeu-se que spams enviados pelos *Heavy senders* e recebidos pelos *Heavy receivers* são considerados mais graves pelo filtro de spam. Logo, apenas com o esforço de identificar esses remetentes e destinatários focos de spam, é possível alcançar resultados significativos para contribuição na economia de recursos e melhoria do desempenho dos provedores de serviços de e-mail durante o tratamento de spams.

Como trabalho futuro pretende-se analisar os impacto da eliminação de usuáros focos de spams que são identificados com a metodologia apresentada neste artigo. Além disso, com posse do log de e-mails legítimos coletado pelo mesmo provedor no mesmo período, pretende-se sobrepor as duas redes formadas (rede de spams e de e-mails legítimos) afim de identificar o motivo porque alguns usuários são mais atacados do que outros e, também, se isso é influenciado por como os spammers decidem os seus alvos, bem como se os usuários se tornam vulneráveis. Tais análises podem ser relevantes para melhoria no desempenho de serviços de mensagens eletrônicas.

Referências

C.E Shannon (1948). A Mathematical Theory of Communication. 27:379–423.

Dan Twining, Matthew M. Williamson, M. J. F. M. M. R. (2004). Email prioritization: reducing delays on legitimate mail caused by junk mail. In *Distributed Computing Systems 2009 ICDCS '09 29th IEEE International Conference on*.

Easley, D. and Jon, K. (2009). *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*. Cambridge University Press, 1nd edition.

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

Gomes, L. H., Almeida, V. A. F., Almeida, J. M., Castro, F. D. O., , and Bettencourt, L. M. A. (2009). Quantifying Social And Opportunistic Behavior In Email Networks. *Advances in Complex Systems*, 12(1):99–112.

Gomes, L. H., Cazita, C., Almeida, J. M., Almeida, V., and Meira, J. W. (2007). Workload models of spam and legitimate e-mails. *Perform. Eval.*, 64(7-8):690–714.

Gomes, L. H., Cazita, C., Almeida, J. M., Almeida, V., and Meira, Jr., W. (2004). Characterizing a Spam Traffic. In *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, pages 356–369, New York, NY, USA. ACM.

Guerra, P. H. C., Guedes, D., Wagner Meira, J., Hoepers, C., Chaves, M. H. P. C., and Steding-Jessen, K. (2010). Exploring the spam arms race to characterize spam evolution. In *Proceedings of the 7th Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS)*, Redmond, WA.

IronPort Email and Web Security (2011). Cisco 2010 annual security report.

Li, F. and Hsieh, M.-H. (2006). An empirical study of clustering behavior of spammers and group-based anti-spam strategies. In *CEAS'06*.

M. E. J. Newman (2006). Power laws, Pareto distributions and Zipfs law. page 28. Department of Physics and Center for the Study of Complex Systems.

Message Labs (2011). Message labs intelligence.

NSS Labs (2010). Consumer anti-malware products group test report.

Nucleus Research (2007). Spam, the repeat offender.

Pathak, A., Jafri, S., and Hu, Y. (2009). The case for spam-aware high performance mail server architecture. In *Distributed Computing Systems, 2009. ICDCS '09. 29th IEEE International Conference on*, pages 155 –164.

Project, T. A. S. (2010). Spamassassin.

Pu, C. and Webb, S. (2006). Observed trends in spam construction techniques: A case study of spam evolution. In *CEAS*.

Ramachandran, A. and Feamster, N. (2006). Understanding the network-level behavior of spammers. *SIGCOMM Comput. Commun. Rev.*, 36:291–302.

Symantec (2011). State of spam e phishing-a monthly report. Technical report.

Trend Micro (2007). InterScan Messaging Security Suite.