VLADIMIR PÍCCOLO BARCELOS

ANÁLISE DE TÉCNICAS DE BAIXO CUSTO COMPUTACIONAL NO COMBATE AO *SPAM*

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Orientador:
Prof. Joaquim Quinteiro Uchôa

LAVRAS
MINAS GERAIS - BRASIL
2009

Ficha Catalográfica preparada pela Divisão de Processos Técnico da Biblioteca Central da UFLA

Barcelos, Vladimir Píccolo.
Análise de técnicas de baixo custo computacional no combate ao *spam* / Vladimir Píccolo Barcelos. – Lavras : UFLA, 2009.
65 p. : il.

Monografia (Graduação) – Universidade Federal de Lavras, 2009.
Orientador: Joaquim Quinteiro Uchôa.
Bibliografia.

1. *E-mail*. 2. *Spam*. 3. *Greylist*. 4. *Blacklist*. 5. Análise de Corpo e Cabeçalho. I. Universidade Federal de Lavras. II. Título.

CDD – 004.692

VLADIMIR PÍCCOLO BARCELOS

ANÁLISE DE TÉCNICAS DE BAIXO CUSTO COMPUTACIONAL NO COMBATE AO *SPAM*

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Aprovada em 18 de junho de 2009

_____
Prof. José Monserrat Neto

_____
Prof. Rêmulo Maia Alves

_____
Prof. Joaquim Quinteiro Uchôa
(Orientador)

LAVRAS
MINAS GERAIS – BRASIL

AGRADECIMENTOS

A Deus por me dar tantas oportunidades.

Aos meus pais pelo incentivo.

A todos os meus amigos, pelo apoio e convivência.

Aos queridos membros da TecnoLivre, pela amizade e compreensão.

Ao Centro de Informática e ao Departamento de Ciência da Computação da Universidade Federal de Lavras que possibilitaram a realização dos trabalhos.

Ao Professor Joaquim pelas orientações.

Sou muito grato a todos.

RESUMO

ANÁLISE DE TÉCNICAS DE BAIXO CUSTO COMPUTACIONAL NO COMBATE AO *SPAM*

Mensagens eletrônicas não solicitadas, conhecidas como *spam,* causam prejuízos tanto aos provedores quanto aos usuários. A utilização de técnicas de baixo custo computacional no combate ao *spam*, principalmente em servidores com muitas contas de usuários, é recomendada para não comprometer o desempenho do serviço. Neste trabalho, objetivou-se avaliar a eficiência única e combinada de três técnicas: *greylist*, *blacklist* e análise de corpo e cabeçalho. Essas técnicas de baixo custo computacional foram aplicadas em um servidor de *e-mail* implementado com *software* livre. Cada técnica ou combinação de técnicas foram aplicadas por um período de uma semana. Altas taxas de filtragem foram obtidas. A eficiência alcançada no combate às mensagens não solicitadas foi de até 94,19%. Esta taxa sugere uma alternativa às técnicas que necessitam de alto poder de processamento para serem executadas.

Palavras-chave: *E-mail*, *Spam*, *Greylist*, *Blacklist*, Análise de Corpo e Cabeçalho.

ABSTRACT

ANALYSIS OF TECHNIQUES OF LOW COMPUTATIONAL COST IN SPAM FILTERING

Unsolicited electronic messages, known as spam, cause several damages to the service providers and to final users. The use of techniques of low computational cost in spam filtering, mainly in servers with many user accounts, is recommended, because they don't compromise the performance of the service. The objective of This paper aims to evaluate the efficiency of three techniques: greylist, body and header message analysis and blacklist. These techniques of low computational cost had been applied in a mail server implemented with free software. Each technique or combination of techniques had been applied by a period of one week. Satisfactory results have been achived. The efficiency reached in unsolicited messages filtering was up to 94,19%. This tax suggests an alternative to the techniques that need high processing to be executed.

Keywords: E-mal, Spam, Greylist, Blacklist, Head Check, Body Check.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

O *e-mail* é um dos meios de comunicação mais práticos e utilizados (Silva, 2007). Tal popularidade foi atingida devido ao seu baixo custo de implementação e alta eficiência. Aproveitando destas facilidades somado à simplicidade do protocolo *Simple Mail Transfer Protocol* (SMTP), milhões de mensagens eletrônicas não solicitadas são enviadas diariamente, causando prejuízos em diversos níveis (Oliveira, 2005). O *spam*, de forma simplificada, é toda mensagem eletrônica não desejada pelo destinatário. Possuem, na maioria das vezes, conteúdo comercial e pode ter o objetivo aplicar golpes em usuários incautos.

A popularização da Internet proporcionou um crescimento exponencial de mensagens eletrônicas não solicitadas. O *spam* tornou-se um problema relevante para os administradores de rede, provedores de Internet e usuários finais. Indivíduos que não possuem filtros anti-*spam,* recebem normalmente grandes quantidades de mensagens não solicitadas. Este usuários perdem muito tempo diferenciando as mensagens válidas das demais, reduzindo a produtividade. Além disso, o *spam* pode fazer com que a quota de armazenamento de um usuário seja extrapolada, impedindo-o de receber mensagens. Por outro lado, o *spam* também consome recursos generalizados da Internet, como banda de transmissão, processamento, armazenamento e outros (Cert.br, 2006).

De acordo com uma pesquisa realizada pela empresa de segurança Sophos (Idgnow, 2009), estima-se que de todos os *e-mails* em circulação na Internet, 97% são *spam*. De acordo com esta referência, o Brasil, além de ser líder na América Latina, também é o segundo maior emissor mundial de *spam*, perdendo apenas para os Estados Unidos.

Em servidores que hospedam centenas ou até milhares de contas de e-mail, é essencial a implantação de técnicas anti-spam. Porém, várias dessas técnicas demandam servidores com alto poder de processamento. De acordo com Hird (2002), analisar cada mensagem em um ambiente onde circulam centenas delas requer grande disponibilidade de recursos. Caso contrário, a entrega das mensagens poderá ser prejudicada. Neste contexto, o administrador deve fazer uso de técnicas que exigem menor processamento, mas que possuam um grau de eficiência aceitável.

1.1. Objetivos

O objetivo do presente trabalho é implementar um servidor de *e-mail*, aplicando e verificando a eficácia de determinadas técnicas no combate ao *spam*. As técnicas utilizadas neste trabalho não exigem grande poder de processamento dos servidores, por isto podem ser consideradas como técnicas de baixo custo computacional. Serão obtidas as eficiências, individual e combinada, das seguintes técnicas: *greylist*, *blacklist* e análise de corpo e cabeçalho.

1.2. Motivação

A impossibilidade de aplicar técnicas como SpamAssassin em um servidor de *e-mail* implementado em uma máquina mais antiga foi a pedra fundamental. Procurar soluções eficientes no combate ao *spam* sem exigir intenso processamento da máquina, beneficiando servidores com baixo poder de processamento ou máquinas com intenso tráfego de mensagens foi a principal motivação para a realização das atividades.

1.3. Organização do Trabalho

Este trabalho é dividido em três partes. Na primeira parte, nos capítulos 2 e 3, é apresentado ao leitor a revisão de literatura sobre o assunto, abordando as mensagens eletrônicas, protocolos, *spam* e seus prejuízos, bem como o funcionamento das técnicas anti-*spam* aplicadas neste trabalho. A segunda parte (capítulo 4) mostra a metodologia aplicada no servidor de *e-mail* durante implementação das técnicas de controle de mensagens não solicitadas. Por fim, os resultados obtidos serão discutidos nos capítulos 5. Conclusões e trabalhos futuros são apresentados no capítulo 6.

2. E-MAIL

Este capítulo aborda os conceitos de *e-mail*, bem como suas partes, sua infra-estrutura de transporte e os protocolos envolvidos neste processo de transmissão. A última subseção descreve brevemente o servidor de *e-mail* Postfix.

E-mail é a abreviação de e*lectronic mail* – correio eletrônico em português. É considerada atualmente como uma das ferramentas digitais de comunicação entre usuários mais populares. Isto se tornou possível devido ao seu baixo custo, tanto financeiro quanto de implementação, além de ser simples e fácil de utilizar.

Cruz (2006) descreve que em 1971, o engenheiro Ray Tomlinson da BBN Technologies[1] desenvolveu um *software* chamado SNDMSG que permitia a transferência de mensagens de texto localmente entre usuários na rede. O mesmo engenheiro criou o símbolo "@", utilizado para indicar que a conta de um usuário encontra-se em um determinado domínio.

Exemplo: laura@bcc.ufla.br, onde:

- **laura** - nome da conta do usuário no determinado servidor
- **@** - este símbolo é lido como "at", que significa "em"
- **bcc.ufla.br** - domínio que hospeda a conta de *e-mail* do usuário.

1 Bolt Beranek and Newman (BBN) Tecnologies – empresa contratada pelo Departamento de Defesa dos Estados Unidos em 1968 para criar a Arpanet, rede de defesa americana, percursora da Internet (BRUM, 2004).

Um ambiente de *e-mail* tem como base a arquitetura cliente-servidor, onde o cliente de *e-mail* proporciona uma interface ao usuário para o envio, recebimento e organização das mensagens e o servidor recebe as mensagens enviadas por clientes de *e-mail* e encaminha ao seu destinatário final.

Tendo em vista a popularização da Internet e consequentemente o aumento exponencial de usuários de seus serviços de comunicação, certos internautas começaram a explorar suas falhas para conseguir algum benefício próprio. Surge então o envio massivo de mensagens não solicitadas, na maioria das vezes contendo códigos ou *links* maliciosos. Este problema será tratado no capítulo 3.

2.1. Infra-estrutura de transporte de mensagens eletrônicas

Oliveira (2005) cita que a infra-estrutura de transporte de *e-mail* é constituída por quatro agentes que funcionam como emissores e/ou receptores de mensagens. São eles:

- *Mail User Agent* (MUA): é um cliente de *e-mail*. É um *software* que permite ao usuário enviar e receber mensagens, bem como gerenciá-las. Normalmente oferecem uma interface amigável ao usuário. O Mozilla Thunderbird[2] é um exemplo de MUA.
- *Mail Transfer Agent* (MTA): é o programa encarregado pelo envio e recebimento das mensagens dos usuários através da rede. Sua função é criar rotas de mensagens, enviar mensagens originadas através dos MUAs e repassar mensagens entre MTAs. O Postfix[3] e Sendmail[4] são

2 http://www.mozilla.com/thunderbird
3 http://www.postfix.org
4 http://www.sendmail.org

exemplos de MTAs.

- *Mail Delivery Agent* (MDA): é o agente que entrega os os *e-mails*. Os MDAs recebem uma mensagem de um MTA e fazem com que esta mensagem seja armazenada ou reencaminhada. O Dovecot[5] é um exemplo de MDA para Linux.
- *Mail Access Agent* (MAA): permite que os MUAs acessem as mensagens que estão na caixa de correio. Esta função é exercida pelos protocolos *Post Office Protocol* (POP) e o *Internet Message Access Protocol* (IMAP).

O agente inteiramente responsável pelo envio e transmissão de *e-mails* entre diferentes usuários é o agente de transporte (POSTEL, 1982). Ele possui crucial finalidade para a efetiva entrega das mensagens de *e-mail*.

Agentes de transporte de *e-mail* tratam a mensagem a ser transportada como um arquivo ASCII[6]. O remetente pode anexar arquivos junto da mensagem, que serão codificados para o formato ASCII pelo cliente de *e-mail*.

2.2. Composição de uma mensagem eletrônica

De acordo com Sica et al. (2003), uma mensagem de *e-mail* é composta por três partes distintas. São elas o envelope, cabeçalho e o corpo. O Antispam.br (2006), um site mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), constitui uma fonte de referência sobre o spam. De acordo com esta

5 http://www.dovecot.org

6 *American Standard Code for Information Interchange* (ASCII) é uma codificação de caracteres de sete *bits* baseada no alfabeto inglês. Desenvolvida a partir de 1960, ainda é base para grande parte das codificações modernas (ELIAS, 2005).

referência, as partes de uma mensagem de *e-mail* serão detalhadas a seguir.

2.2.1. Envelope

O envelope contém as informações necessárias para que o MTA receptor de uma mensagem saiba o que fazer com ela. No protocolo SMTP o envelope é construído a partir dos comandos MAIL FROM e RCPT TO.

O MAIL FROM contém o remetente da mensagem. O MTA pode utilizar este endereço para enviar uma mensagem de erro em caso de falha na entrega da mensagem. Já o RCPT TO contém um ou mais destinatários da mensagem.

2.2.2. Cabeçalho

Diversos campos compõem o cabeçalho de uma mensagem de *e-mail*. Tais campos contém informações tanto para o MTA quanto para o MUA, e podem ter o conteúdo acrescentado pelo MUA e pelos vários MTAs utilizados para entregar a mensagem. Alguns dos campos do cabeçalho são:

- **Return-Path**: é o endereço para onde o MTA deve entregar a mensagem de erro. Normalmente o conteúdo deste campo é copiado do envelope (MAIL FROM).
- **Received**: indica a procedência (pelo endereço IP), a data e a hora em que a mensagem foi recebida e, eventualmente, a auto identificação do transmissor (HELO/EHLO). Analisando os vários campos Received: é possível verificar o caminho que a mensagem percorreu antes de ser entregue. Porém só é realmente confiável o Received: mais recente, pois

ele foi inserido pelo MTA que está sob o controle do administrador.

- **From**: designa o remetente nominal da mensagem, que não é necessariamente igual ao que aparece no envelope ou no campo Return-Path:.
- **To: / Cc: / Bcc**: campos opcionais, designam os destinatários que não necessariamente coincidem com os declarados no envelope. O campo To: recebe um ou mais destinatários da mensagem; Já o campo Cc: recebe os endereços que irão receber uma cópia da mensagem; Por fim, o Bcc: contém os destinatários que receberão uma cópia da mensagem, porém este campo é invisível aos destinatários.

Os campos From: e To: podem não conter o remetente e o destinatário verdadeiro da mensagem. O usuário deve ser criterioso ao clicar em *links* ou abrir arquivos de mensagens suspeitas.

2.2.3. Corpo

O corpo da mensagem é separado pelo cabeçalho por uma linha e contém todo o conteúdo da mensagem em si. Os campos Content-type:, Content-Transfer-Encoding: e MIME-Type descrevem a codificação da mensagem em caso de mensagem complexas.

Em 13 de agosto de 1982 foi publicado uma padronização para a estrutura das mensagens de *e-mail*, desenvolvida pelo *Internet Engineering Task Force* – IETF. Esta primeira versão recebeu a nomenclatura RFC 822 (CROCKER, 1982), e na sua última atualização, em outubro de 2008, a nomenclatura RFC 5322 (RESNICK, 2008).

```
Delivered-To: vpbarcelos@gmail.com
Received: by 10.151.50.5 with SMTP id c5cs240763ybk;
        Thu, 30 Apr 2009 07:22:20 -0700 (PDT)
Received: by 10.224.45.129 with SMTP id e1mr1880688qaf.15.1241101340432;
        Thu, 30 Apr 2009 07:22:20 -0700 (PDT)
Return-Path: <vladimir@bcc.ufla.br>
Received: from mail.bcc.ufla.br ([200.131.251.203])
                                by    mx.google.com    with    ESMTP    id
27si3427825qyk.53.2009.04.30.07.22.18;
        Thu, 30 Apr 2009 07:22:18 -0700 (PDT)
Received-SPF: neutral (google.com: 200.131.251.203 is neither permitted
nor denied by best guess record for domain of vladimir@bcc.ufla.br)
client-ip=200.131.251.203;
Authentication-Results:     mx.google.com;     spf=neutral     (google.com:
200.131.251.203 is neither permitted nor denied by best guess record for
domain of vladimir@bcc.ufla.br) smtp.mail=vladimir@bcc.ufla.br
Received: by mail.bcc.ufla.br (Postfix, from userid 48)
       id DC99B14464C; Thu, 30 Apr 2009 11:22:14 -0300 (BRT)
To: vpbarcelos@gmail.com
Subject: Mensagem de teste
MIME-Version: 1.0
Date: Thu, 30 Apr 2009 11:22:14 -0300
From: =?UTF-8?Q?Vladimir_P=C3=ADccolo_Barcelos?= <vladimir@bcc.ufla.br>
Message-ID: <c176a27759af0c50f9706c9a5a2971c9@pcl.bcc.ufla.br>
X-Sender: vladimir@bcc.ufla.br
User-Agent: RoundCube Webmail/0.2
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset="UTF-8"


Exemplo de e-mail.
```

Figura 2.1: Exemplo de uma mensagem de *e-mail*.

Durante todo o processo de composição, envio, tráfego, armazenagem e entrega de uma mensagem eletrônica, diversos protocolos são envolvidos. Estes protocolos serão descritos a seguir. Porém, uma visão geral de todo o processo pode ser visualizado na Figura 2.2.

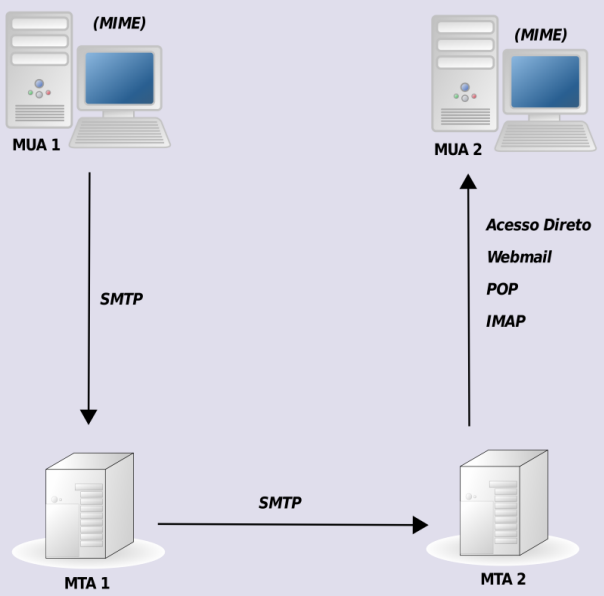

Figura 2.2: Agentes envolvidos desde a composição até a entrega de uma mensagem de *e-mail*. Fonte: Uchôa (2005).

2.3. Protocolos de Transferência de Mensagens Eletrônicas

2.3.1. *Simple Mail Transfer Protocol* – SMTP

O advento da Internet e o início de sua popularização na década de 80, exigiu uma padronização nos diversos sistemas de troca de mensagens eletrônicas. Os sistemas em operação até então eram, na maioria das vezes, inoperantes ou incompatíveis entre si. Publicou-se em 13 de agosto de 1982 o *Simple Mail Transfer Protocol* (SMTP) – Protocolo Simples para Transferência de Correio. Tal protocolo foi primeiramente publicado com a nomenclatura RFC 821 (POSTEL, 1982), sendo atualizado em abril de 2001 recebendo a

nomenclatura RFC 2821 (KLENSIN, 2001).

O modelo de transmissão de *e-mail* adotado pelo SMTP pode ser visto de acordo com a Figura 2.3:

Figura 2.3: Modelo de transmissão do protocolo SMTP. Fonte: Postel (1982).

O objetivo do SMTP é transferir mensagens entre usuários de forma confiável e eficiente. Conforme sua especificação, este protocolo é independente do subsistema de transmissão em particular e requer somente um canal de transmissão de dados eficiente (KLENSIN, 2001).

Silva (2007) diz que basicamente, o mecanismo de transmissão do protocolo SMTP é o modelo cliente-servidor. Ao iniciar a transmissão de uma mensagem, o cliente estabelece uma conexão bidirecional com o servidor SMTP, que por padrão utiliza o protocolo de transporte *Transmission Control Protocol* (TCP), e o servidor recebe conexões, geralmente na porta 25. Uma vez estabelecida a conexão, o cliente transmite a mensagem para o servidor ou se ocorrer alguma falha, reporta ao remetente.

O protocolo SMTP não determina se a mensagem deve ser entregue ao servidor local ou a outro servidor remoto de SMTP. O programa cliente SMTP é o responsável por pesquisar o servidor de *e-mail* de destino, geralmente, através do protocolo TCP/IP, resolvendo o nome através de consulta ao registro *Mail*

eXchanger (MX) do servidor *Domain Name System* (DNS) responsável pelo domínio de destino.

Uma importante função deste protocolo é a capacidade de transmitir mensagens diretamente ao destinatário final ou a um "*relay*" intermediário, isto é, ele pode assumir o papel de um cliente SMTP depois de receber alguma mensagem; ou "*gateway*", isto é, ele pode transportar a mensagem recebida utilizando um protocolo diferente do SMTP.

2.3.2. *Post Office Protocol* – POP

O *Post Office Protocol* (POP) é um protocolo utilizado por clientes de *e-mail* (MUAs) para baixar mensagens de *e-mail* de um servidor remoto através de uma conexão TCP/IP geralmente na porta 110. Atualmente encontra-se na versão 3 (POP3) e está definido no RFC 1939 (MYERS et al., 1996). Este protocolo permite que os MUAs faça o *download* das mensagens do servidor MTA para a máquina local. Só após este processo o usuário poderá manipular suas mensagens de *e-mail* sem a necessidade de estar conectado integralmente ao MTA.

Segundo Myers et al. (1996), o protocolo POP3 funciona resumidamente da seguinte forma:

- Uma conexão entre o MUA e o MTA é estabelecida através do protocolo TCP/IP;
- O MUA autentica no MTA;
- As mensagens de *e-mail* existentes na caixa de correio do usuário são transferidas em sequência para a máquina local do usuário;
- As mensagens são apagadas da caixa de correio do usuário no servidor

(é possível mantê-las no servidor, mas o usuário deverá selecionar esta opção nas configurações do MUA).

- Finaliza a conexão com o servidor;
- O usuário pode ler e manipular as mensagens localmente em sua máquina.

Com o POP3, a conexão é necessária somente quando o MUA está transferindo as mensagens do MTA. A leitura e manipulação das mensagens podem ser realizadas sem a necessidade de uma conexão ativa. Isto pode ser uma vantagem aos usuários que pagam pelo tempo de conexão. Por outro lado, o usuário necessita descarregar completamente a mensagem do servidor para poder visualizá-la. Caso a mensagem contenha grandes arquivos anexados, o usuário deverá esperar vários minutos para ter acesso a mensagem.

2.3.3. *Internet Message Access Protocol* – IMAP

O *Internet Message Access Protocol* (IMAP) também é um protocolo utilizado por clientes de *e-mail* (MUAs) para baixar mensagens de *e-mail* de um servidor remoto através de uma conexão TCP/IP geralmente na porta 143. Atualmente encontra-se na versão 4 revisão 1 (IMAP4rev1) e é definido pelo RFC 3501 (CRISPIN, 2003).

Através deste protocolo o usuário acessa e manipula suas mensagens e pastas de sua conta *e-mail* diretamente no servidor (CRISPIN, 2003). Como as mensagens ficam armazenadas remotamente, o usuário tem a vantagem de ter acesso às suas mensagens independente do computador que utiliza. Este protocolo fornece ao usuário um acesso mais rápido às suas mensagens além de

permitir e múltiplos acessos simultâneos à mesma caixa de mensagem.

Mesmo sendo um protocolo mais avançado que o POP3, o usuário na maioria das vezes possui um limite de espaço no servidor para armazenar as mensagens. Além disso, é necessário estar integralmente conectado ao servidor durante todo o processo de leitura e manipulação das mensagens.

2.4. Postfix

O Postfix é um servidor de *e-mail* que originou-se em 1997 no Centro de Pesquisa Thomas J. Watson com o nome de VMailer (VENEMA, 2008). Foi concebido por Wietse Zweitze Venema, enquanto trabalhava, para a International Business Machines Corp. (IBM). Venema é mais conhecido pelos programas que escreveu para proteger sistemas contra intrusos, como o Security Administrator Tool for Analyzing Networks (SATAN) e TCP Wrapper (ELIAS, 2005).

De acordo com Elias (2005), a proposta do VMailer era ser um servidor de *e-mail*, seguro, rápido, fácil de ser configurado e ser compatível o suficiente com o Sendmail, o que facilitaria a migração. O funcionamento do VMailer seria baseado em uma coleção de pequenos programas, relativamente simples e rápidos, que em conjunto fariam todo o trabalho de um servidor de *e-mail*. Esta abordagem é diferente do Sendmail, que é um grande programa monolítico com uma linguagem de configuração e programação bastante confusa e complexa.

O VMailer passou a se chamar Postfix em dezembro de 1998, quando a IBM e Wietse Zweitze Venema liberaram o código do VMailer na Internet (ELIAS, 2005).

A administração do MTA Postfix é relativamente simples. Basicamente, toda sua configuração se resume em dois arquivos: o main.cf e o master.cf, localizados normalmente no diretório /etc/postfix (VENEMA, 2008). O usuário

deverá possuir permissões de administrador para alterar estes arquivos.

3. SPAM

Este capítulo aborda os conceitos básicos de *spam,* seus prejuízos, os diferentes tipos, os mecanismos envolvidos no processo de envio destas mensagens além de algumas técnicas utilizadas para combatê-las.

Spam é o termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *Unsolicited Commercial E-mail*)" (CERT.BR, 2006).

A palavra "*spam*" originou-se da marca de um tipo de carne suína enlatada da Hormel Foods Corporation cuja denominação é ***Sp****iced H****am***. Esta carne foi utilizada em um quadro de TV[7] do grupo de humoristas ingleses chamado Monty Phyton, onde uma garçonete descrevendo o cardápio repetia sempre a palavra *Spam*, pois todos os pratos vinham acompanhados dele. Um grupo de *vikings* da mesa ao lado começa a cantar insistentemente: "*Spam*, amado S*pam*, glorioso S*pam*, maravilhoso S*pam*!", impossibilitando qualquer tipo de conversa (HAMBRIDGE e LUNDE, 1999). Este quadro foi montado para ironizar o racionamento de comida ocorrido na Inglaterra durante e após a Segunda Guerra Mundial. O *Spam* foi um dos poucos alimentos excluídos desse racionamento, o que eventualmente levou as pessoas a enjoarem do alimento.

Apesar da existência de mensagens não-eletrônicas que podem ser comparadas ao *spam*, como por exemplo folhetos promocionais não solicitados, o termo é reservado aos meios eletrônicos (OLIVEIRA, 2005).

De acordo com Templeton (2003), um dos primeiros casos reportados de *spam* aconteceu em maio de 1978. Neste ano um funcionário da DEC, uma empresa americana pioneira na indústria da computação, foi

7 O quadro pode ser assistido em: http://www.youtube.com/watch?v=3kjdrl6qjwY

contratado para fazer propaganda do novo sistema DEC 20. Ele enviou então uma mensagem sobre este sistema à vários usuários da rede Arpanet.

Porém, uma mensagem promovendo *Green Cards* enviada em 1994 para diversos grupos de discussão é batizada oficialmente como a primeira mensagem de *spam* (ANTISPAM.BR, 2006).

3.1. Os Prejuízos do *spam*

O *spam* é um problema que causa prejuízos em todos os níveis da Internet, desde o provedor do serviço até ao usuário. Cert.br (2006) detalha abaixo os danos causados pelas mensagens eletrônicas não solicitadas aos usuários do serviço de correio eletrônico:

- **Não-recebimento de *e-mails*** – Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Conforme o número de *spams* recebidos, o usuário corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, todas as mensagens enviadas a partir desse momento serão devolvidas ao remetente e o usuário não receberá *e-mails* até que possa liberar espaço em sua caixa postal.
- **Gasto desnecessário de tempo** – Para cada *spam* recebido, o usuário necessita gastar um determinado tempo para ler, identificar o *e-mail* como *spam* e removê-lo da caixa postal.
- **Aumento de custos** – Independentemente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do *spam* é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à Internet, cada *spam* representa custo da ligação que ele pagará.

- **Perda de produtividade**. – Para quem utiliza o *e-mail* como ferramenta de trabalho, o recebimento de *spams* aumenta o tempo gasto com a leitura de *e-mails.* Há também a possibilidade de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.
- **Conteúdo impróprio ou ofensivo** – Como a maior parte dos *spams* são enviados para conjuntos de endereços de *e-mail*, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.
- **Prejuízos financeiros causados por fraude** – O *spam* tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas neste tipo de mensagem fraudulenta.

Já os prejuízos causados aos provedores de acesso ou ao setor de informática de uma empresa também são descritos a seguir também pelo Cert.br (2006):

- **Impacto na banda** – Para as empresas e provedores, o volume de tráfego gerado por causa de *spams* obriga a aumentar a capacidade de seus *links* de conexão com a Internet. Como o custo dos *links* é alto, isto diminui os lucros do provedor e poderá refletir no aumento dos custos para o usuário.
- **Má utilização dos servidores** – Os servidores de *e-mail* dedicam boa parte do seu tempo de processamento para tratar das mensagens não

solicitadas. Além disso, o espaço em disco ocupado por mensagens não solicitadas enviadas para um grande número de usuários é considerável.

- **Inclusão em listas de bloqueio** – O provedor que tenha usuários envolvidos em casos de *spam* pode ter sua rede incluída em listas de bloqueio. Esta inclusão pode prejudicar o recebimento de *e-mails* por parte de seus usuários e ocasionar a perda de clientes.
- **Investimento em pessoal e equipamentos** – Para lidar com todos os problemas gerados pelo *spam*, os provedores necessitam contratar mais técnicos especializados, comprar equipamentos e acrescentar sistemas de filtragem de *spam*. Como consequência, os custos do provedor aumentam.

3.2. Tipos de *spam*

O conteúdo do *spam* pode ser propaganda de produtos e serviços, pedido de doações para obras assistenciais, correntes da sorte, propostas de ganho de dinheiro fácil, boatos desacreditando o serviço prestado por determinada empresa, dentre outros (TEIXEIRA, 2001). Dependendo deste conteúdo e do objetivo pretendido pelo emissor de *spam* (*spammer*), a mensagem não solicitada pode receber diversas classificações. Os tipos mais comuns são expostos nas subseções seguintes.

3.2.1. Propagandas

Mensagens com conteúdo de propaganda são conhecidos como UCE (*Unsolicited Comercial E-mail*). Este tipo de *spam* normalmente promovem medicamentos sem prescrição, *software* pirata ou ilegal, diplomas universitários,

produtos eróticos, páginas da internet, entre outros. Este é o tipo mais antigo de *spam* e foi responsável em média por 92,82% de todas as mensagens de *spam* circuladas na Internet durante o mês de maio de 2009 (TRACELABS, 2009).

Na maioria das mensagens, o produto ou serviço oferecido contém alguma característica ilegal. Na maioria das mensagens, o *spammer* ou a empresa emissora também são desconhecidos do público. Alguns *spams* oferecem produtos que não existem ou serviços que nunca serão entregues. Os casos mais comuns são os *e-mails* vendendo pílulas milagrosas para melhorar o desempenho sexual de homens e mulheres ou, ainda, para perder peso dormindo (ANTISPAM.BR, 2006).

3.2.2. Correntes (*chain letters*)

Spams classificados como correntes contam uma história ou ensinam alguma simpatia. É comum encontrar apresentações eletrônicas anexadas à estas mensagens. Em suma, promovem sorte, saúde ou riqueza àqueles que repassarem a mensagem para o maior número possível de pessoas. Além disso, costumam "amaldiçoar" os leitores que quebrarem a corrente, ou seja, os que não passam a mensagem à diante. Desta forma, elas têm a capacidade de atingir um número exponencial de pessoas em um curto período de tempo. Atualmente, o envio em massa de correntes diminuiu bastante, continuando frequente apenas em grupos e listas de discussão entre amigos (ANTISPAM.BR, 2006).

3.2.3. Boatos (*hoaxes*)

Boatos diferem-se das correntes pelo seu conteúdo. O primeiro geralmente conta histórias alarmantes e falsas ou notícias sensacionalistas de

caráter duvidoso, fazendo com que o leitor fique sensibilizado e propague a mensagem para o maior número possível de usuários. Estas mensagens normalmente são difamatórias ou filantrópicas.

Mensagens difamatórias possuem conteúdo que denigre empresas ou produtos, prometem falsos brindes ou retratam dos riscos que um determinado componente da fórmula de um produto pode causar à saúde. Já os boatos filantrópicos contam histórias de pessoas doentes, em estágio terminal, informando que se o *e-mail* não for repassado, a família não receberá ajuda em dinheiro de alguma organização.

Boatos famosos são frequentemente divulgados. Isto acontece devido à grande quantidade de novos usuários na Internet que, por falta de informação ou de experiência, repassam os boatos antigos, iniciando um novo ciclo de propagação (ANTISPAM.BR, 2006).

3.2.4. Ameaças, brincadeiras e difamação

O simples fato de se enviar uma mensagem para um grande número de pessoas já caracteriza o *spam*. Neste contexto, existem casos de pessoas que enviam mensagens contendo ameaças, brincadeiras inconvenientes ou difamação de amigos, familiares, ex-namorados(as), ex-esposos(as), entre outros (SILVA, 2007).

A vítima envolvida neste tipo de *spam* que se sentir prejudicada poderá registrar um Boletim de Ocorrência e, eventualmente, conduzir algum processo judicial contra o emissor reunindo todas as provas necessárias.

3.2.5. Pornografia

O envio de material pornográfico por meio de mensagens não solicitadas também é considerada uma das modalidades mais antigas de *spam*. Porém, este tipo necessita de atenção especial. Afinal, crianças podem ser receptoras destas mensagens. Por isto, recomenda-se atenção especial dos responsáveis por crianças que tem acesso a serviços de *e-mail*. No mês de maio de 2009, uma média de 2,45% dos *spams* foram classificados como de conteúdo adulto (TRACELABS, 2009). Além disto, os *links* contidos neste tipo de *spam* são 280 vezes mais clicados do que os contidos em mensagens que vendem produtos farmacêuticos (MINDLIN, 2006). Ainda de acordo com esta referência, cerca de 5,6% dos usuários que recebem mensagens de conteúdo pornográfico clicam nos *links*.

3.2.6. Códigos maliciosos

Esta categoria compreende as mensagens que tem como objetivo final a propagação de códigos maliciosos (*malwares*), que executam ações maliciosas em um computador. Diversos destes códigos são inseridos em *e-mails*, contendo textos que tentam convencer o usuário a executar o código malicioso em anexo.

Em geral, estes códigos também são utilizados em *spams* enviados por golpistas e fraudadores. Os *malwares* utilizam-se de diversas formas para furtar dados de um usuário. As mais comuns são capturar teclas digitadas no teclado ou sobrepor a janela do navegador do usuário com uma janela falsa, onde os dados serão coletados e enviados ao fraudador (ANTISPAM.BR, 2006).

3.2.7. Fraudes

Obter acesso aos dados confidenciais de um usuário ou de uma empresa é uma tarefa difícil. Desta forma, os *spammers* utilizam-se de abordagens que exploram falhas de seguranças para realizar fraudes financeiras. Através de um texto convincente e se passando por alguma instituição financeira, os *spammers* tentam persuadir o usuário a fornecer seus dados pessoais confidenciais.

O *phishing* foi um termo atribuído à mensagens não solicitadas que se passam por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular. Estas mensagens realizam estelionato, através da instalação de algum código malicioso que monitora a máquina e capturam dados do usuário ou através do acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários (ANTISPAM.BR, 2006).

3.2.8. *Spit* e *Spim*

Os termos *spit* e *spim* significam respectivamente "*spam via Internet Telephony*" e "*spam via Instant Messenger*". Apesar de não serem estritamente *e-mails*, são mensagens eletrônicas enviadas sem solicitação. O *spit* são mensagens enviadas para telefones IP, ou programas de voz sobre IP (VoIP). Já o *spim*, são mensagens enviadas para programas de mensagem instantânea como o MSN Messenger, ICQ ou Yahoo! Messenger.

3.2.9. *Spam* via redes de relacionamento

Redes de relacionamento pessoal, como Orkut, Myspace, Twitter e Facebook são terrenos férteis para a divulgação de *spams*. Como o número de usuários ativos nestes serviços é alto, os *spammers* apostam no grande alcance

de mensagens entre os usuários. Porém, a maioria destes serviços possuem ferramentas para bloquear mensagens de pessoas que o usuário não conhece.

3.3. Mecanismos envolvidos no envio de *e-mails* não solicitados

As técnicas utilizadas pelos *spammers* têm como principais objetivos enganar os mecanismos anti-*spam* e atingir o maior número possível de destinatários. O processo de envio de *spams* é dividido em três etapas: a coleta de dados, a formatação das mensagens e o envio da mensagem.

A fase de coleta dos dados consiste em obter o maior número possível de endereços eletrônicos e criar uma lista de destinatários de *spam*. Os endereços de *e-mail* de usuários são adquiridos pelos *spammers* de diversas maneiras. Os destinatários são capturados em mensagens da Usenet[8], de listas de *e-mail*, ou através de pesquisas na *web*. Para que a coleta seja eficiente e tenha um custo reduzido, o procedimento é totalmente automatizado através de um *software* chamado robô. Este software também pode ser chamado de *bot*. Os *bots*, por exemplo, acessam uma página a procura de endereços eletrônicos analisando o conteúdo desta página e repete o procedimento a cada nova página que acessa. Outra forma bastante comum é a obtenção de endereços de máquinas infectadas por vírus ou outras pragas.

Após o advento de mecanismos anti-*spams* que analisam conteúdo, a formatação das mensagens de *spams* passou a receber maior importância (TAVIEIRA, 2008). As primeiras mensagens de *spam* não se preocupavam com

8 Usenet (do inglês *Unix User Network*) surgiu em 1979 e é um meio de comunicação onde usuários discutem assuntos separados por tipos (chamados de *newsgroups* ou grupos de notícias). Os artigos postados nos *newsgroups* são retransmitidos através de uma extensa rede de servidores interligados entre si (JUNIOR, 2008).

o seu conteúdo, sendo facilmente identificadas ao se verificar determinadas palavras no corpo da mensagem, como por exemplo: “viagra”, “cialis”, etc. Assim, para tentarem contornar os mecanismos anti-*spam* baseados em análise de conteúdo, os *spammers* passaram a usar a técnica chamada de *Snowalking Messages* onde são inseridas nas mensagens diversas palavras ou frases retiradas de textos legítimos. Esta técnica gera um texto aleatório sem nenhuma ligação com o objetivo principal do *spam* e, portanto, o mecanismo de análise por conteúdo pode acabar sendo enganado, deixando de classificar a mensagem como *spam*.

Uma decisão importante no número de destinatários efetivos dos *spams* é a opção por mensagens no formato texto ou no formato HTML. A versatilidade do formato HTML é usada pelos *spammers* para tornar mais difícil a análise do conteúdo do texto por parte dos mecanismos anti-*spam*. Além destes formatos, o uso de figuras está se tornando comum em *spams*, onde a propaganda está contida dentro de uma figura, tornando difícil a análise do texto da imagem, sendo necessário um processo de reconhecimento de caracteres com maior custo computacional. Cert.br (2006) afirma que o envio do *spam* é a fase final. Uma técnica amplamente utilizada pelos *spammers* para enviar mensagens é o abuso de servidores de *e-mail* vulneráveis ou mal configurados. Estes servidores, também chamados de *open relay*, permitem o envio de mensagens originadas de qualquer remetente, de qualquer rede (OLIVEIRA, 2005). Os *spammers* usam estes servidores para enviar milhares de mensagens.

Segundo Tavieira (2008), a maior parte das mensagens não solicitadas é enviada a partir de redes de máquinas zumbis, também chamadas de *botnets*. Essas redes são compostas por diversas máquinas infectadas por um vírus ou outra praga. Estas máquinas zumbis se conectam a um servidor que as comanda. Desta forma o *spammer* utiliza máquinas de usuários comuns para enviar

mensagens. Utilizando esta técnica de envio, os *spammers* garantem que suas mensagens não serão bloqueadas por listas negras, pois além da entrega ser distribuída, os zumbis enviam uma menor quantidade de mensagens do que um servidor dedicado.

3.4. Técnicas de combate ao *spam*

Atualmente existem diversas técnicas de combate ao *spam*, cada uma com diferentes abordagens e custos computacionais. As principais são baseadas em listas de servidores confiáveis e não confiáveis, ou na filtragem das mensagens baseadas em seu conteúdo. Tais técnicas estão relacionadas com a habilidade do servidor em distinguir mensagens verdadeiras dos *spams*. Neste trabalho, algumas técnicas de baixo custo computacional serão analisadas. Estas técnicas recebem tal denominação pois o servidor receptor utiliza-se de pouco processamento na filtragem das mensagens. As técnicas utilizadas neste trabalho serão abordadas a seguir.

3.4.1. Greylist

Harris (2003) afirma que o *greylist,* pode ser considerado como uma leve arma contra mensagens não solicitadas. Seu funcionamento enquadra-se no meio termo entre o *whitelist* (mensagens destes remetentes são permitidas) e *blacklist,* (remetentes cujas mensagens não são permitidas).

Esta técnica parte dos princípios de que *e-mails* válidos são enviados a partir de MTAs legítimos (que possuem políticas de retransmissão em caso de erros temporários e mantém filas) e que a maioria dos *spammers* não utilizam de um MTA legítimo para enviar suas mensagens. O protocolo SMTP é considerado

um protocolo de transporte não-confiável, portanto, a possibilidade de falhas temporárias estão embutidas no núcleo do protocolo. O conceito de *greylisting* consiste em recusar temporariamente uma mensagem de um remetente desconhecido e esperar por sua retransmissão.

Existem *spammers* que utilizam MTAs legítimos ou mesmo reenviam as mensagens a fim de contornar esta técnica. Ainda assim, o *greylisting* tem se mostrado eficiente para barrar mensagens enviadas por máquinas zumbis infectadas por vírus e outras pragas virtuais (ANTISPAM.BR, 2006).

Segundo Dias e Uchôa (2005), um *spammer* normalmente utiliza um sistema de entrega de mensagens que desprezam as mensagens de erro dos destinatários. Como eles enviam para milhares de endereços, receber e tratar eventuais mensagens de erro dos destinatários custariam muito, seja em largura de banda quanto em processamento.

Em um servidor de *e-mail* com *greylist* implementado, a mensagem de um remetente desconhecido é colocada em espera. Então, um erro temporário é enviado pelo protocolo SMTP ao remetente, solicitando o reenvio da mensagem. Normalmente, o MTA de um *spammer* não processa as mensagens de erros, portanto não realiza uma nova tentativa de entrega da mensagem ao destinatário.

Um MTA com *greylisting* implementado respeita as seguintes regras do diagrama apresentado na Figura 3.1:

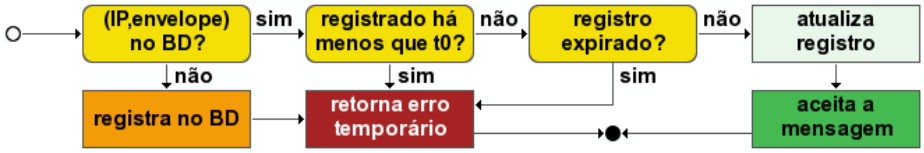

Figura 3.1: Regras de um MTA com *greylisting* implementado. Fonte: Antispam.br (2006).

Se o remetente da mensagem encontra-se registrado no banco de dados

do MTA, a mensagem é aceita. Caso contrário ela não é entregue durante um intervalo de espera (t0) e uma mensagem de erro temporário é retornada ao emissor. Caso o MTA emissor seja válido, o mesmo irá retransmitir a mensagem. Após o intervalo de tempo t0, caso a mensagem continue a ser retransmitida pelo MTA, a mesma é aceita. Caso contrário, o registro é removido do banco de dados após o intervalo de tempo t1. A Figura 3.2 ilustra este processo.

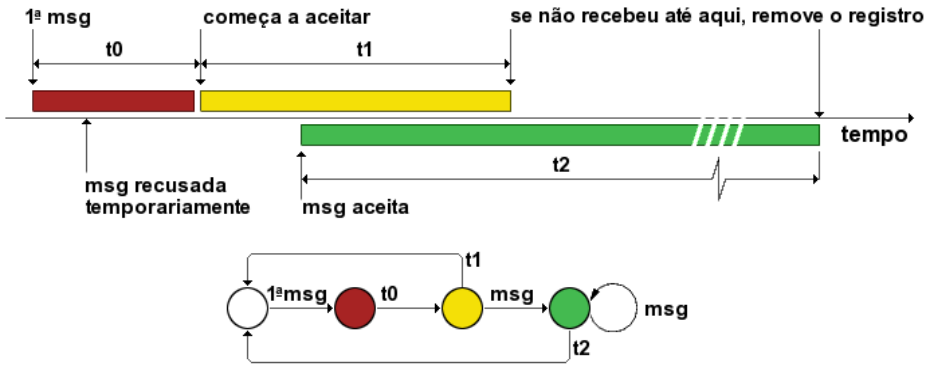

Figura 3.2: Processo do *greylist* para aceitar ou recusar uma mensagem recebida. Fonte: Antispam.br (2006).

Em geral as implementações de *greylisting* mantém um banco de dados com registros indexados por endereço IP da origem, endereço do remetente no envelope e pelo endereço do destinatário no envelope (ANTISPAM.BR, 2006).

Repare que uma mensagem é barrada por *greylist* antes mesmo do servidor destinatário recebê-la. Desta forma, esta técnica não exige intenso processamento dos servidores.

3.4.2. Blacklist

Um dos primeiros sistemas anti-*spam* existentes era baseado na

utilização de listas negras, que são listas contendo endereços de *e-mail* ou de IP de remetentes que são comprovadamente emissores de *spam*. Nas listas brancas são colocados os endereços confiáveis, considerados não emissores de *spam*. Ao receber mensagens, o MTA checa na lista negra se o endereço do remetente está contido. Caso estiver, a mensagem é ignorada imediatamente e uma mensagem de erro é enviada ao emissor. Caso a mensagem não esteja contida na lista negra consultada, o servidor pode permitir a entrega ou executar uma nova checagem da mensagem utilizando alguma outra técnica, caso o servidor estiver configurado para tal operação.

Inicialmente, essas listas eram feitas pelos próprios usuários e cada um ficava responsável por adicionar e remover os endereços das duas listas. Isso demandava um grande esforço do usuário, pois ele tinha que separar as mensagens e determinar se o endereço deveria ser colocado na lista branca, na negra ou, em caso de dúvidas, em nenhuma das duas listas. A evolução natural foi tornar o sistema centralizado, onde entidades centrais controlam a adição e remoção de endereços das listas.

A primeira implementação desse tipo de sistema distribuído, de acordo com Tavieira (2008), foi chamada de *Realtime Blackhole List* (RBL), criado por Paul Vixie. Na RBL eram listados os endereços IP de máquinas emissoras de *spam*. Esta lista era atualizada manualmente. Após a RBL, surgiu a *Open Relay Behavior-modification System* (ORBS) cuja principal diferença para a RBL é a realização automática de testes para identificar servidores que permitem o envio de mensagens de *spam*. O IP dos servidores considerados *open relay* são adicionados automaticamente na lista negra. Caso o administrador de tal servidor queira retirar seu IP desta lista negra, o mesmo deverá contactar a entidade que mantém a lista solicitando a remoção.

O processo de consulta a estas listas distribuídas é geralmente feita

através do protocolo *Domain Name System* (DNS), fazendo com que elas sejam chamadas genericamente de *Domain Name System Black Lists* (DNSBLs). Para realizar a consulta a estas listas, o servidor que recebeu a mensagem verifica se o endereço IP do cliente ou de outro servidor que se conectou a ele está presente na lista DNSBL configurada. A verificação utilizando o protocolo DNS é realizada fazendo uma consulta DNS ao endereço formado invertendo-se os *bytes* do endereço IP do cliente e adicionando o nome do domínio da entidade responsável pela DNSBL.

Como qualquer técnica anti-*spam*, o *blacklist* pode estar sujeita a falsos negativos. Isto acontece quando o endereço IP de algum servidor é incorretamente adicionado à lista. Isto pode acontecer quando máquinas são infectadas por vírus e *spammers* abusam destas máquinas para enviar mensagens. Neste caso, o endereço desta máquina pode entrar em listas negras e mensagens válidas provenientes do usuário desta máquina podem ser recusada pelos demais servidores com a técnica implementada.

As listas negras são consideradas um bloqueio bastante efetivo de mensagens não solicitadas. Estudos mostram que até 80% dos *spams* podem ser evitados por meio do uso desses mecanismos (TAVIEIRA, 2008).

3.4.3. Análise de Corpo e Cabeçalho

Assim como as outras técnicas mencionadas, a análise de corpo e cabeçalho das mensagens pode ser ativadas no arquivo de configuração do MTA.

Cada linha do cabeçalho ou do corpo da mensagem é comparada com uma lista de padrões, definida pelo administrador do servidor de *e-mail*. Caso obtenha sucesso nesta comparação, uma ação especificada é executada. Este

processo de comparação é então repetido para as linhas de cabeçalho e corpo das próximas mensagens. Este processo não decodifica arquivos anexos ou descompactam arquivos (VENEMA, 2008).

Através desta técnica, o administrador de rede consegue barrar mensagens que contenham uma determinada palavra ou frase, tanto no campo assunto quanto em seu conteúdo. É possível impedir o recebimento de mensagens de um determinado remetente ou de um determinado domínio. Pode-se também configurar o servidor para impedir a entrega de mensagens que contenham arquivos de extensões suspeitas, que possam conter vírus. A checagem do conteúdo não é realizada. Simplesmente são rejeitadas as mensagens que contenham arquivos com determinadas extensões.

Por ser altamente configurável, as taxas de filtragem podem ser altas, obtendo maior eficiência. Mas o administrador precisa implementar esta técnica de forma equilibrada, para não obter falsos negativos, ou seja, deve evitar que mensagens válidas sejam barradas por este sistema. Infelizmente nenhuma técnica está livre de falsos negativos.

3.5. Outras técnicas de combate ao *spam*

Nesta sessão serão citadas algumas técnicas anti-*spam* existentes mas que não foram aplicadas neste trabalho.

3.5.1. AMaViS

De acordo com Amavis (2004), *A Mail Virus Scanner* (AMaViS) é um software anti-vírus de mensagens eletrônicas para sistemas baseados em UNIX.

É um *software* livre, implementado juntamente ao servidor de e-mail. Mensagens com anexos infectados são limpos ou excluídos, dependendo da configuração adotada pelo administrador. Como existe uma quantidade considerável de mensagens não solicitadas com algum anexo malicioso, o AMaViS é capaz de filtrar a maioria das mensagens contendo anexos infectados e algumas mensagens de *spam*.

3.5.2. SpamAssassin

SpamAssassin é um software licenciado através da licença Apache que filtra as mensagens consideradas como *spam*.

Segundo Antispam.br (2006), o software analisa o conteúdo das mensagens recebidas e as classifica com pontos (*score*). Quando maior a pontuação atribuída à mensagem, maior a chance de ela ser considerada como *spam*. Normalmente, se a pontuação for maior que 5, a mensagem é classificada como *spam*. Esta mensagem pode ser movida para uma pasta "spam" ou ter seu assunto iniciando com "***SPAM***", dependendo da configuração do sistema pelo administrador. Caso a mensagem receba uma pontuação menor que 5, a mensagem é considerada válida e deixada na pasta de entrada do usuário. Esta técnica pode utilizar em seu método de classificação, algorítimos bayesianos.

Esta técnica exige intenso processamento do servidor, pois cada mensagem é analisada por completo.

3.5.3. *Sender Policy Framework* – SPF

Sender Policy Framework (SPF) é um sistema que evita que domínios da Internet enviem e-mails não autorizados se passando por outro domínio.

Segundo Ellermann (2008), o SPF verifica no cabeçalho da mensagem se o servidor de e-mails utilizado para enviar a mensagem, está autorizado na relação de IP's que respondem pelo domínio do remetente. Também informa se o domínio autoriza ou não que outros IP's fora desta relação enviem e-mails em seu nome.

Esta configuração é realizada na entrada TXT da zona de DNS seguindo as regras da RFC 4408 (WONG e SCHLITT, 2006). Caso este sistema esteja ativo e o IP solicitado seja diferente dos autorizados, o e-mail será rejeitado.

3.5.4. Filtros Bayesianos

De acordo com Antispam.br (2006), os filtros Bayesianos implementam um algoritmo de probabilidade baseado na Teorias de Bayes.

Softwares que utilizam esses filtros precisam passar por um período de treinamento, no qual tratam conjuntos de mensagens legítimas e também mensagens que conhecidamente são spam, criando uma base de dados inicial com informações sobre as ocorrências de palavras em cada um dos casos. Passado o período de treinamento, o programa vai ficando mais eficiente na filtragem de mensagens não solicitadas. O consumo de recursos computacionais é elevado, porém menos crítico que no caso dos antivírus, mas mesmo assim pode ser comprometedor em servidores de alto tráfego.

Para que o filtro se adapte ao caráter mutável do spam é necessário que o treinamento do filtro seja contínuo, com a identificação dos spams que não foram classificados e das mensagens que não são spam e que foram rotuladas como tal (ANTISPAM.BR, 2006).

Como os filtros Bayesianos podem acarretar falsos positivos, é aconselhável não descartar uma mensagem marcada como spam, mas sim optar

por colocá-la em quarentena. Esse problema pode ser agravado caso a base de dados com que ele toma decisão for desatualizada ou baseada em outro idioma.

4. METODOLOGIA

Nos capítulos anteriores, foram abordados o *e-mail*, a problemática das mensagens eletrônicas não solicitadas, e algumas técnicas de combate que exigem baixo custo computacional. No presente trabalho, foi implementado um servidor de *e-mail* para a testar, de forma isolada e combinada, a eficiência das técnicas *greylist*, *blacklist* e análise de corpo e cabeçalho.

A máquina utilizada para a realização dos trabalhos possui as seguintes configurações:

- Processador: Intel Core 2 Duo, 2.2 GHz, FSB 800
- Memória RAM: 2 GB, DDR2 667 MHz
- Disco rígido: 40 GB, interface PATA.
- Leitor e Gravador de DVD

O sistema operacional instalado na máquina foi a distribuição Linux Fedora 10 arquitetura x86_64 com kernel versão 2.6.27-11-generic. O serviço de *e-mail* foi implementado utilizando a versão 2.2.5 do MTA Postfix, a versão 1.1.7 do MDA Dovecot e o Mysql versão 5.0.67 para a criação de contas de usuário virtuais.

O servidor foi hospedado no domínio bcc.ufla.br, que não estava sendo utilizado pelo Departamento de Ciência da Computação (DCC) da Universidade Federal de Lavras (UFLA). A utilização deste domínio foi importante, pois enquanto ativo, ele fornecia os serviços de hospedagem *web*, servidor de arquivos, além do servidor de *e-mail* com diversas contas de usuários.

Com a finalidade de manipular, interpretar e gerar estatísticas dos *logs* do servidor de *e-mail*, o aplicativo Advanced Web Statistics (Awstats) versão 6.9

build 1.925 foi instalado na máquina em questão.

4.1. Contas de *e-mail*

Para a criação das contas de *e-mail*, tomou-se o cuidado de não escolher nomes que eram utilizados enquanto o DCC/UFLA administrava o domínio. Tal medida foi tomada para respeitar a privacidade dos antigos usuários que ainda poderiam eventualmente receber alguma mensagem de *e-mail* caso tivessem suas antigas contas reativadas.

Como dito no capítulo anterior, para criar uma lista de destinatários, os *spammers* utilizam-se de programas (*bots*), que percorrem páginas da Internet capturando endereços de *e-mail*. Pensando nisto, uma página *web* fictícia foi criada para divulgar as contas de *e-mail* utilizada nos testes (Figura 4.1). Para hospedar esta página, a versão 2.2.10 do servidor Apache foi instalada.

No total foram criadas quinze contas de *e-mail*. Destas, cinco foram divulgadas amplamente na Internet: na página *web* criada, em grupos de discussão, bate-papos, comentários de *blogs*, ou qualquer site que fornecesse alguma forma de cadastro de *e-mail*. Nomes simples de usuários foram escolhidos para estas cinco contas principais. As dez contas restantes foram expostas apenas em uma página *web* secundária, chamada "Contatos", hospedada no domínio em uso. Um *link* na página principal fornece acesso à esta página secundária.

Optou-se em limitar a divulgação das dez das contas de *e-mail* desta forma para testar se as mesmas seriam descobertas por possíveis *bots*.

Após a ativação do serviço de *e-mail*, um período de quatro semanas foi gasto na divulgação das cinco contas de *e-mail* principais. O período em questão compreendeu-se entre 16 de fevereiro e 16 de março de 2009.

As cinco contas de e-mail principais, amplamente divulgadas, foram: laura@bcc.ufla.br, vladimir@bcc.ufla.br, brenda@bcc.ufla.br, fernandes@bcc.ufla.br, e pereira@bcc.ufla.br.

As dez contas secundárias criadas foram: sac@bcc.ufla.br, juridico@bcc.ufla.br, secretaria@bcc.ufla.br, analise@bcc.ufla.br, infraestrutura@bcc.ufla.br, in-frent@bcc.ufla.br, expotic@bcc.ufla.br, byte-foto@bcc.ufla.br, soft-mega@bcc.ufla.br e empretools@bcc.ufla.br.

Figura 4.1: Página *web* do domínio www.bcc.ufla.br, desenvolvida unicamente para divulgar as contas de *e-mail* fictícias utilizadas nos trabalhos.

4.2. Implementação das técnicas

Quatro semanas após a implantação do servidor de *e-mail*, encerrava-se o período de divulgação das cinco contas principais. Após este período, cada conta recebia uma média de duzentas mensagens de *spam* por dia. Deu-se então início a aplicação das técnicas. Estas foram aplicadas durante sete semanas, no período entre 30 de março e 17 de maio de 2009.

Cada técnica ou combinação de técnicas permaneceu ativa durante o período de sete dias, conforme a Tabela 4.1. Nas semanas onde aplicaram-se duas ou mais técnicas, é possível observar que o *greylisting* precedeu o *blacklisting* durante as filtragens; sendo a análise de corpo e cabeçalho a última técnica a ser aplicada.

Tabela 4.1: Cronograma de aplicação das técnicas de controle de *spam*.

Semanas	Técnicas
Semana 1 (30/03 a 05/04)	*Greylist*
Semana 2 (06/04 a 12/04)	*Blacklist*
Semana 3 (13/04 a 19/04)	Análise de Corpo e Cabeçalho
Semana 4 (20/04 a 26/04)	*Greylist* + *Blacklist*
Semana 5 (27/04 a 03/05)	*Greylist* + Análise de Corpo e Cabeçalho
Semana 6 (04/05 a 10/05)	*Blacklist* + Análise de Corpo e Cabeçalho
Semana 7 (11/05 a 17/05)	*Greylist* + *Blacklist* + Análise de Corpo e Cabeçalho

4.2.1. Greylist

O *greylist* foi implementado, instalando o Postgrey versão 1.31 no servidor. O Postgrey é um serviço de *greylisting* para Postfix. Utilizou-se o gerenciador de pacotes *yum* para a instalação do mesmo. O prazo de espera antes da efetiva aceitação de mensagens provenientes de remetentes desconhecidos foi configurado em cinco minutos. Se após este período o remetente continuar realizando tentativas de entrega, a mensagem é aceita.

Para a integração do Postgrey no Postfix, a seguinte linha foi adicionada ao *smtpd_recipient_restrictions* do arquivo de configuração main.cf do Postfix:

```
smtpd_recipient_restrictions = check_policy_service
unix:postgrey/socket
```

4.2.2. Blacklist

Para a implantação de *blacklisting* no servidor, a seguinte linha foi adicionada ao *smtpd_client_restrictions* do arquivo de configuração main.cf do Postfix:

```
smtpd_client_restrictions =  reject_rbl_client
zen.spamhaus.org, reject_rbl_client bl.spamcop.net
```

É possível ver que as listas negras utilizadas neste servidor foram a zen.spamhaus.org e bl.spamcop.net. A primeira lista, é uma combinação de todas as listas disponíveis pela Spamhaus (instituição que procura e cadastra os *spammers*). Assim, as requisições podem ser concentradas em uma única lista, diminuindo o tempo das consultas. A lista SpamCop foi fundada em 1998 por Julian Haight e compreende uma ampla lista de IP reportados aos moderadores

da lista.

Quando o Postfix recebe uma requisição para entregar uma mensagem a um usuário local, o remetente desta mensagem é checado no primeiro serviço de lista negra configurada. Caso o remetente não esteja cadastrado, o mesmo é checado na segunda lista. Se o remente for encontrado, em qualquer lista que seja, a entrega é imediatamente abortada e não é realizada nenhuma outra checagem.

4.2.3. Análise de Corpo e Cabeçalho

No Postfix, esta checagem é implementada adicionando as seguintes linhas no arquivo main.cf:

```
header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
```

Estas linhas informam que o Postfix deve realizar cada checagem seguindo as regras em um determinado arquivo de expressões regulares.

A linha *header_checks* habilita o Postfix a checar o cabeçalho das mensagens de acordo com o arquivo de texto header_checks localizado dentro da pasta /etc/postfix. Neste arquivo, as regras são incuídas pelo administrador do serviço para impedir a entrega de mensagens. O Postfix realiza a comparação do cabeçalho da mensagem a ser entregue com as regras do arquivo de expressões regulares. Caso alguma comparação for positiva, a mensagem é imediatamente descartada e nenhuma outra checagem é realizada.

Já a linha *body_checks* compara o conteúdo do corpo da mensagem de acordo com as regras cadastradas no arquivo de texto body_checks localizado em /etc/postfix. Caso o conteúdo do corpo da mensagem a ser entregue obedeça

alguma regra do arquivo, a mensagem não é entregue e nenhuma outra checagem é realizada.

5. RESULTADOS E DISCUSSÃO

O servidor de *e-mail* foi efetivamente ativado no dia 16 de fevereiro de 2009. Desde então iniciou-se o processo de divulgação na Internet das cinco contas de *e-mail* principais. Esta tarefa foi finalizada no dia 16 de março.

No momento em que o servidor entrou em atividade, foi possível identificar que algumas mensagens já estavam sendo enviadas para o domínio em uso. Estas mensagens eram destinadas aos antigos usuários, datados da época em que o domínio era administrado pelo DCC/UFLA.

A Figura 5.1 apresenta o gráfico com o número total de mensagens efetivamente entregues às contas de *e-mail* durante o período precedente ao da aplicação das técnicas anti-*spam*.

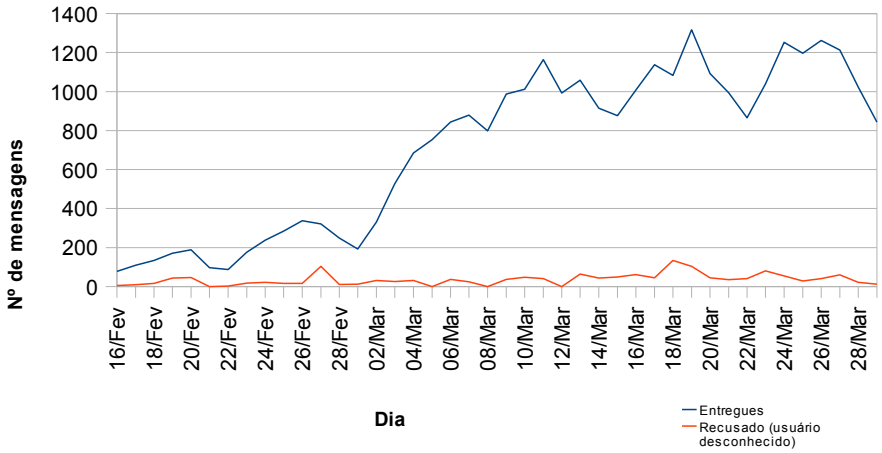

Figura 5.1: Número total de mensagens de *e-mail* do servidor *bcc.ufla.br* no período que precede a aplicação das técnicas anti-*spam.*

Durante esses 42 dias, 1.508 mensagens não foram entregues pois o destinatário era desconhecido. Isto proporciona uma média de 36,78 mensagens

não entregues por dia. É possível perceber que durante os finais de semana, principalmente aos domingos, há uma perceptível diminuição do número de mensagens recebidas.

Nos treze dias compreendidos entre o fim da divulgação das contas de *e-mail* e o início da aplicação das técnicas, o servidor manteve uma média de 1.101,31 mensagens recebidas por dia. Este número, se dividido entre as cinco contas de *e-mail* principais, obtém-se uma média diária de 220 mensagens.

Como as contas de usuário são fictícias (não pertencem a usuários reais), todas as mensagens recebidas nestas contas foram consideradas como *spam*.

Como dito anteriormente, dez das quinze contas de *e-mail* criadas foram apenas divulgadas em uma página *web* secundária hospedada no servidor. Estas contas começaram a receber mensagens não solicitadas a partir do dia 8 de abril, 51 dias após a ativação do servidor de *e-mail*. O número total de *spams* recebidos nestas dez contas foi de 184, valor pequeno se comparado ao recebido pelas contas divulgadas. Este fato pode levar à inferência de que é bastante provável que qualquer endereço de *e-mail* exposto em uma página da Internet por um período razoável de tempo pode ser alvos de *spams*. Ressalta-se que nenhum cálculo estatístico foi realizado para testar esta inferência.

Somando todas as contas, nos 91 dias de execução do trabalho, 47.436 mensagens de *e-mail* foram efetivamente entregues; 2.586 mensagens não foram entregues pois o destinatário era desconhecido; 14.225 mensagens foram rejeitadas pela da técnica *greylisting*; o *blacklisting* bloqueou 15.743 mensagens e 11.733 mensagens foram filtradas pela análise do corpo e do cabeçalho das mensagens.

O Anexo A mostra trechos do *log* do servidor de e-mail retratando as etapas ocorridas desde o pedido de entrega até a rejeição de uma mensagem de *e-mail* por cada uma das três técnicas aplicadas neste trabalho.

5.1. Técnica 1: *Greylist*

Entre os dias trinta de março e cinco de abril de 2009 a técnica *greylisting* foi aplicada. A Tabela 5.1 mostra a quantidade de mensagens efetivamente entregues e as bloqueadas pelo Postgrey. As Figuras 5.2 e 5.3 mostram o desempenho do Postgrey e a relação de mensagens bloqueadas.

Tabela 5.1: Número total de mensagens bloqueadas e recebidas pelo servidor durante a aplicação do *greylist.*

Mensagens	Número Total
Bloqueadas pelo Postgrey	2.901
Efetivamente entregues	5.194
Total de mensagens:	8095

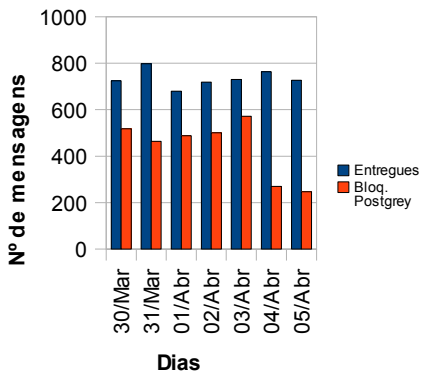

Figura 5.2: Número total de mensagens entregues e rejeitadas pelo sistema durante a aplicação do *greylisting.*

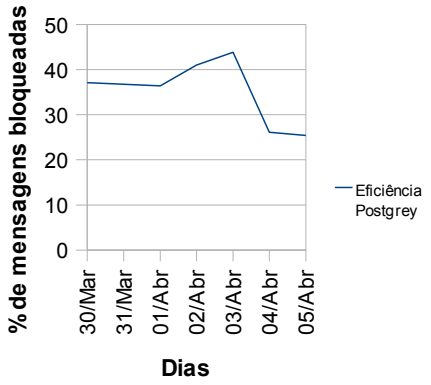

Figura 5.3: Eficiência geral do *greylisting* no bloqueio de mensagens eletrônicas não solicitadas.

Aplicando o *greylist* de maneira isolada, não foi possível obter altas taxas de filtragem. Em média, apenas 35,21% das mensagens foram bloqueadas.

Segundo Antispam.br (2006), o *greylisting* tem se mostrado eficiente para barrar mensagens enviadas por vírus, máquinas zumbis ou outras pragas virtuais. Através de uma análise do conteúdo das mensagens recebidas, foi constatado um baixo número de *spams* provenientes dessas fontes. Isto explica a baixa eficácia do *greylist* aplicado isoladamente neste sistema. Porém, após a aplicação desta técnica, o número de mensagens contendo códigos maliciosos foram reduzidos a zero.

Em seus trabalhos, Dias e Uchôa (2005) conseguiram reduzir o número de mensagens recebidas no servidor em mais de 60% utilizando o Postgrey. Analisando ainda o conteúdo das mensagens, detectaram uma redução de 97,38% de *spam* de um único usuário de seus servidores.

Comparando os dados de Dias e Uchôa (2005) com os obtidos neste trabalho, pode-se concluir que atualmente, alguns *spammers* já são capazes de burlar o *greylisting*. Durante a aplicação desta técnica, foi observado que os *spammers* enviaram uma mesma mensagem para o mesmo grupo de destinatários duas ou mais vezes, enganando o *greylist*. Esta suspeita foi levantada pois algumas mensagens de *spam* foram recebidas repetidamente, duas ou mais vezes, em um curto período de tempo. É provável também que os *spammers* estejam utilizando servidores de *e-mail* legais, bem implementados e que processam as mensagens de erro dos destinatário, reenviando a mensagem para um destinatário que a rejeitou.

5.2. Técnica 2: *Blacklist*

Entre os dias 6 e 12 de abril de 2009, foi aplicada a técnica de filtragem de mensagens por lista negra. A Tabela 5.2 mostra o número de mensagens bloqueadas e efetivamente entregues durante a aplicação desta técnica.

Tabela 5.2: Número total de mensagens bloqueadas e recebidas pelo servidor durante a aplicação do *blacklisting*.

Mensagens	Número Total
Bloqueadas pela zen.spamhaus.org	4.786
Bloqueadas pela bl.spamcop.net	114
Total de mensagens bloqueadas	4.900
Mensagens efetivamente entregues	3.216
Total	8.116

Diariamente, esta técnica bloqueou em média 60,56% das mensagens eletrônicas não solicitadas. A lista zen.spamhaus.org foi responsável por 97,67% dos bloqueios. Já a lista bl.spamcop.net bloqueou apenas 2,33% de todas as mensagens. Isto deve-se ao fato de que a lista mantida pela Spamhaus foi configurada primariamente no sistema, ou seja, todas as checagens eram realizadas primeiramente nesta lista. Caso a mensagem fosse reprovada, ela era ignorada imediatamente, interrompendo outras checagens. As Figuras 5.4 e 5.5 apresentam os dados coletados durante esta segunda fase do trabalho.

Devido ao grande volume de mensagens recebidas nas cinco contas principais, uma análise mais profunda de todas foi inviável. Porém, analisando uma conta em específico, foi possível verificar uma drástica redução das mensagens não solicitadas de conteúdo promocional, principalmente aquelas que promovem algum produto farmacêutico.

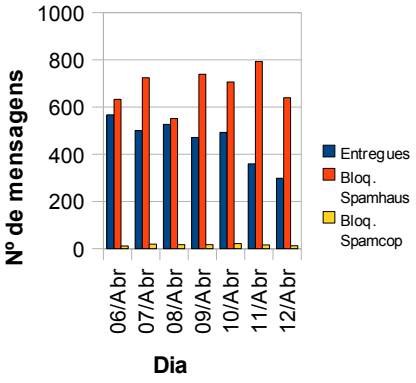

Figura 5.4: Número total de mensagens entregues e rejeitadas pelo sistema durante a aplicação do *blacklisting*.

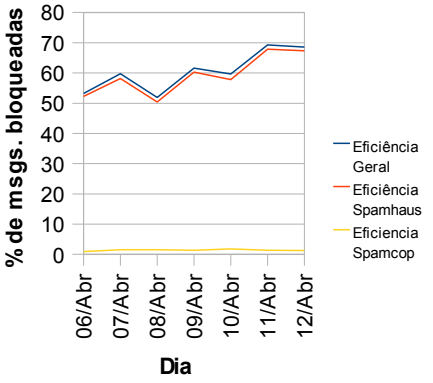

Figura 5.5: Eficiência das listas negras no bloqueio de mensagens eletrônicas não solicitadas.

5.3. Técnica 3: Análise de corpo e cabeçalho

Esta técnica consistiu em filtrar as mensagens tomando como base uma lista programada pelo administrador do sistema. Caso o assunto, ou o corpo da mensagem contenha alguma palavra ou frase contida na lista programada, a mensagem é imediatamente rejeitada. Também é possível rejeitar a mensagem caso a mesma contenha algum determinado tipo de anexo.

Mensagens contendo arquivos anexos e extensões de risco foram rejeitadas. Assim como as palavras-chave mais comuns em mensagens de *spam*.

A Tabela 5.3 mostra o número de mensagens bloqueadas e recebidas durante a aplicação desta técnica. A Figura 5.6 mostra o gráfico representando o número de mensagens entregues e rejeitadas. A Figura 5.7 mostra a eficiência obtida com a aplicação desta técnica.

Tabela 5.3: Número total de mensagens bloqueadas e recebidas pelo servidor durante a filtragem por análise de corpo e cabeçalho.

Mensagens	Número Total
Bloqueadas por análise de corpo e cabeçalho	5.306
Efetivamente entregues	2.422
Total	7.728

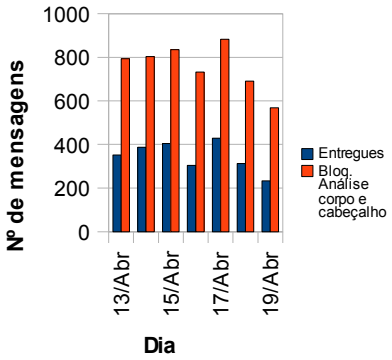

Figura 5.6: Número total de mensagens entregues e rejeitadas pelo sistema durante a filtragem por análise de corpo e cabeçalho.

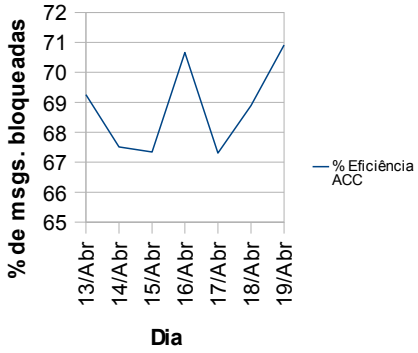

Figura 5.7: Eficiência geral da filtragem de mensagens não solicitadas através da análise do corpo e cabeçalho.

Nesta terceira fase, uma média diária de 68,84% de mensagens foram rejeitadas. Não foi possível obter melhores resultados pois uma grande parte dos *spams* recebidos não continham textos (apenas imagens), prejudicando esta checagem. Além disso, algumas mensagens de *spam* estavam escritas em outros idiomas que não o inglês e português. Estas mensagens não foram bloqueadas pois o arquivo usado na filtragem das mensagens possuía palavras-chave apenas nestes dois idiomas.

5.4. Técnica 4: *Greylist + Blacklist*

Nesta quarta fase do trabalho, uma combinação das técnicas *greylist* e *blacklist* foi aplicada. Em média, cerca de 71,63% das mensagens foram bloqueadas diariamente.

A Tabela 5.4, bem como as Figuras 5.8 e 5.9 mostram o comportamento do servidor de *e-mail* nesta etapa do trabalho. Isoladamente, o *greylist* bloqueou 42,05% de todas as mensagens e o *blacklist* foi responsável por rejeitar 29,58% de todas as mensagens.

Acredita-se que o número de mensagens bloqueadas só não foi maior nesta etapa pois as contas de *e-mail* receberam diversas mensagens não solicitadas provenientes de lojas verdadeiras. Lojas reconhecidas possuem um servidor de *e-mail* bem configurado, capaz de reenviar uma mensagem caso o destinatário negue o recebimento.

Tabela 5.4: Número total de mensagens bloqueadas e recebidas pelo servidor durante a aplicação combinada do *greylisting* e *blacklisting*.

Mensagens	Número Total
Bloqueadas pelo Postgrey	3.526
Bloqueadas pelas listas-negra	2.472
Total de mensagens bloqueadas	5.998
Mensagens efetivamente entregues	2.377
Total	8.375

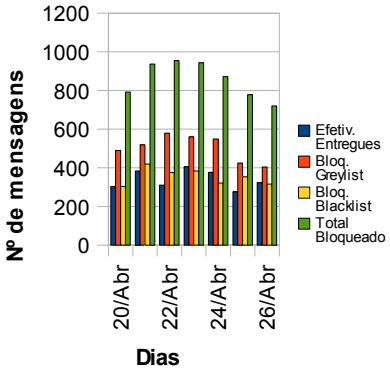

Figura 5.8: Número total de mensagens entregues e rejeitadas pelo sistema durante a aplicação combinada do *greylisting* e *blacklisting*.

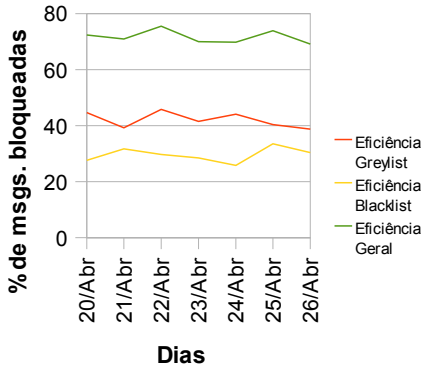

Figura 5.9: Eficiência da combinação das técnicas de *greylisting* e *blacklisting* na filtragem de mensagens não solicitadas.

5.5. Técnica 5: *Greylist* + Análise de corpo e cabeçalho

Nesta etapa do trabalho, foi possível bloquear em média cerca de 74,33% das mensagens por dia. O *greylist* foi responsável por impedir o recebimento de 41,68% das mensagens enquanto a análise de corpo e cabeçalho rejeitou 32,65%.

A Tabela 5.5 e as Figuras 5.10 e 5.11 ilustram o comportamento de filtragem das mensagens durante a aplicação das duas técnicas em questão.

Tabela 5.5: Número total de mensagens bloqueadas e recebidas pelo servidor durante a aplicação combinada de *greylisting* e análise de corpo e cabeçalho.

Mensagens	Número Total
Bloqueadas pelo Postgrey	3.751
Bloqueadas por análise de corpo e cabeçalho	2.930
Total de mensagens bloqueadas	6.682
Mensagens efetivamente entregues	2.322
Total	9.004

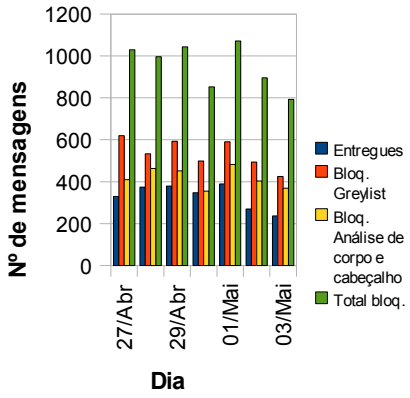

Figura 5.10: Número total de mensagens entregues e rejeitadas pelo sistema durante a aplicação combinada do *greylisting* com a filtragem por análise de corpo e cabeçalho.

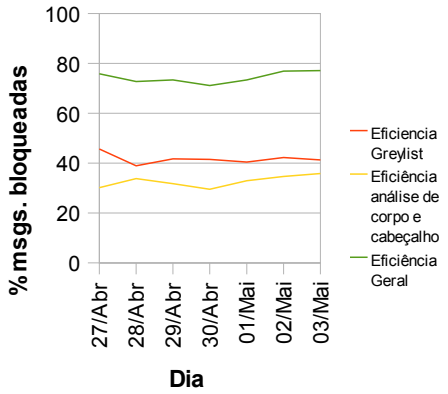

Figura 5.11: Eficiência da combinação das técnicas de *greylisting* e análise de corpo e cabeçalho na filtragem de mensagens não solicitadas.

5.6. Técnica 6: *Blacklist* + análise de corpo e cabeçalho

Nesta penúltima etapa de combinação de técnicas, foi possível bloquear diariamente uma média de 80,95% das mensagens recebidas. As listas negras

impediram o recebimento de 57,99% das mensagens e a análise de corpo e cabeçalho bloquearam cerca de 22,96%.

A Tabela 5.6 mostra o número de mensagens bloqueadas e recebidas durante a aplicação desta técnica. A Figura 5.12 mostra o gráfico representando o número de mensagens entregues e rejeitadas. A Figura 5.13 mostra a eficiência obtida com a aplicação desta técnica.

Tabela 5.6: Número total de mensagens bloqueadas e recebidas pelo servidor durante a aplicação combinada de *blacklisting* e análise de corpo e cabeçalho.

Mensagens	Número Total
Bloqueadas por *blacklist*	4.836
Bloqueadas por análise de corpo e cabeçalho	1.887
Total de mensagens bloqueadas	6.723
Mensagens efetivamente entregues	1.587
Total	8.310

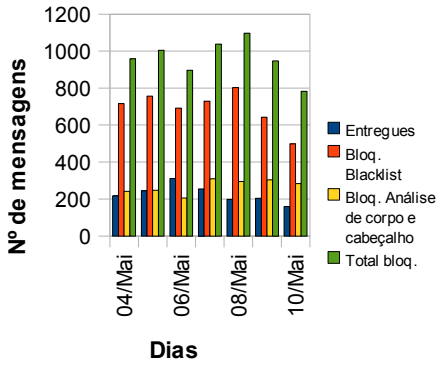

Figura 5.12: Número total de mensagens entregues e rejeitadas pelo sistema durante a aplicação combinada do *blacklisting* com análise de corpo e cabeçalho.

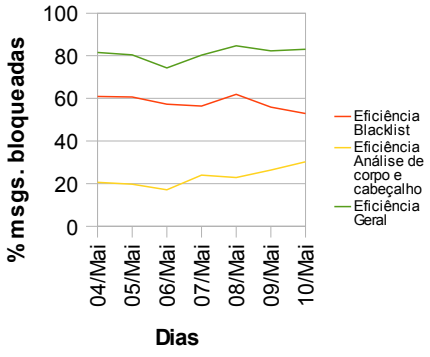

Figura 5.13: Eficiência da combinação das técnicas *blacklisting* e análise de corpo e cabeçalho na filtragem de mensagens não solicitadas.

5.7. Técnica 7: *Greylist* + *Blacklist* + Análise de corpo e cabeçalho

Na última etapa do trabalho, as três técnicas estudadas foram aplicadas simultaneamente. Desta forma, foi possível obter uma média diária de 94,19% de mensagens bloqueadas. O *greylisting* foi responsável por rejeitar 40,68% das mensagens. O *blacklisting* impediu o recebimento de 36,69% de mensagens e a análise de corpo e cabeçalho foi responsável por bloquear 16,82% de todas as mensagens.

A Tabela 5.7 mostra os números totais de mensagens recebidas e bloqueadas por cada uma das técnicas nesta combinação, bem como o total geral dessas mensagens.

As Figuras 5.14 e 5.15 mostram a eficiência de cada uma das técnicas, bem como a contribuição de cada uma no combate das mensagens não solicitadas.

Tabela 5.7: Número total de mensagens bloqueadas e entregues aplicando simultaneamente as técnicas *greylisting*, *blacklisting* e análise de corpo e cabeçalho.

Mensagens	Número Total
Bloqueadas por *greylist*	3.891
Bloqueadas por *blacklist*	3.535
Bloqueadas por análise de corpo e cabeçalho	1.610
Total de mensagens bloqueadas	9.036
Mensagens efetivamente entregues	569
Total	9.605

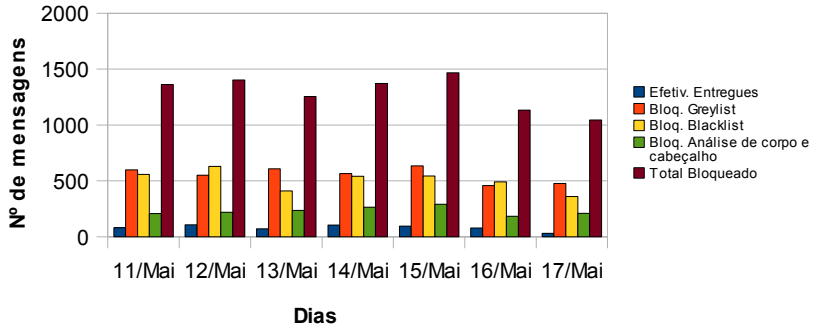

Figura 5.14: Número total de mensagens entregues e rejeitadas pelo sistema durante a aplicação combinada de *greylisting*, *blacklisting* e análise de corpo e cabeçalho.

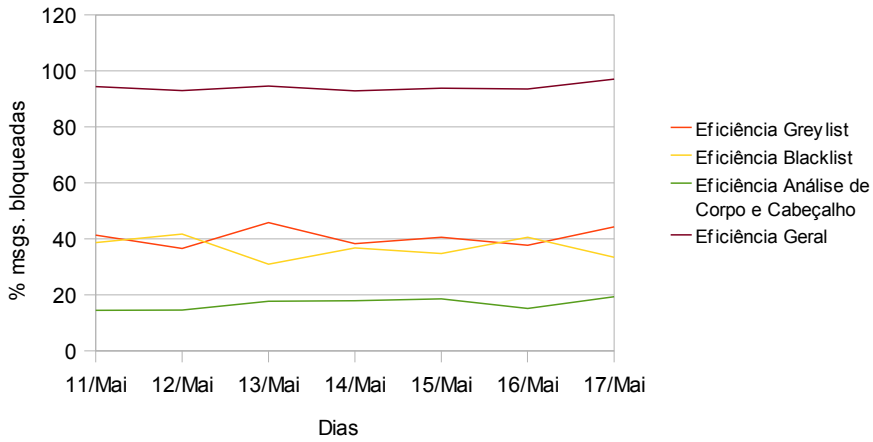

Figura 5.15: Eficiência da combinação das técnicas de *greylisting, blacklisting* e análise de corpo e cabeçalho na filtragem de mensagens não solicitadas.

É possível perceber que a taxa de bloqueio geral alcançada com a combinação destas técnicas é bastante aceitável. Durante a aplicação destas técnicas e analisando as mensagens de uma das cinco contas principais, verificou-se que as mensagens com conteúdo de vírus e outros códigos maliciosos foram reduzidas a zero. Além disso, a maioria das mensagens de *spam* recebidas eram provenientes de lojas brasileiras reconhecidas além de

mensagens escritas em outros idiomas que não o inglês.

6. CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho, objetivou-se implementar um servidor de e-mail e aplicar algumas técnicas de baixo custo computacional na filtragem de *spam*. Diante dos resultados obtidos, entre sete repetições, a que apresentou o melhor resultado foi a combinação das três técnicas simultâneas. Foi obtido 94,19% de eficiência no combate de mensagens não solicitadas, um valor bastante aceitável.

É possível combater mensagens não solicitadas com técnicas menos agressivas em se tratando de processamento. Com os resultados obtidos, principalmente na última repetição, pode-se sugerir uma eventual migração ou aplicação destas técnicas em servidores com baixo poder computacional e/ou máquinas com intenso fluxo de mensagens.

A técnica de análise de corpo e cabeçalho é a única que necessita de uma manutenção do administrador de rede. O conteúdo da lista utilizada para filtrar as mensagens pode eventualmente se tornar obsoleto, prejudicando a eficiência ou filtrando mensagens legítimas (falsos negativos).

É preciso ressaltar que nenhuma técnica anti-*spam* está imune aos falsos negativos. Apesar de não se ter relatado nenhum deste incidente durante a execução deste trabalho, recomenda-se ao administrador maior cautela ao adotar diversas técnicas. Todas as técnicas adotadas em um sistema de filtragem de *spam* devem estar bem configuradas para um funcionamento correto e saudável do ambiente de *e-mail*.

Como trabalhos futuros, sugere-se aplicar as técnicas de *greylist*, *blacklist* e análise de corpo e cabeçalho, ou a combinação delas, em um servidor de *e-mail* real, com contas de usuários válidas. Assim será possível observar o real comportamento em relação as mensagens válidas e as não solicitadas.

Pode-se realizar também uma análise estatística em relação aos falsos positivos, se existirem. Pode-se também realizar uma comparação estatística da eficiência das três técnicas abordadas neste trabalho com outras, de alto custo computacional.

Referências Bibliográficas

AMAVIS – **A Mail Virus Scanner**, 2004. Site da Internet. Disponível em: <http://www.amavis.org>. Acesso em: 19 de junho de 2009.

ANTISPAM.BR **Estrutura da Mensagem**. 2006. Disponível em: <http://www.antispam.br/admin/>. Acesso em: 19 de junho de 2009.

BRUM, M. A. C. **O Uso do E-mail como Ferramenta de Marketing**, 2004. Colóquio Internacional sobre a Escola Latino-Americana de Comunicação - CELACOM. São Paulo, SP. Disponível em: <http://encipecom.metodista.br/mediawiki/index.php/O_uso_do_e-mail_como_ferramenta_de_marketing>. Acesso em: 03 de fevereiro de 2009.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil **Cartilha de Segurança para Internet, Parte IV: Spam**. Versão 3.1. 2006. Disponível em: <http://cartilha.cert.br>.

CRISPIN, M. **Internet MEssage Access Protocol - Version 4rev1**. Março, 2003. Disponível em: <http://www.faqs.org/ftp/rfc/pdf/rfc3501.txt.pdf>. Acesso em: 24 de abril de 2009.

CROCKER, D. H. **RFC 822 - Standard for the Format of Arpa Internet Text Messages**. Agosto, 1982. Disponível em: <http://www.faqs.org/ftp/rfc/pdf/rfc822.txt.pdf>. Acesso em: 12 de maio de 2009.

CRUZ, G. D. O E-mail e sua Produção no Meio Eletrônico: O Suporte Afeta o Gênero? **Revista Letra Magna - Revista Eletrônica de Divulgação Científica em Língua Portuguesa, Lingüística e Literatura**. ano 03, n. 05, 22 p. 2º Semestre de 2006.

DIAS, S. P.; UCHÔA, J. Q. **Uso de Greylists e Controle de Relays Abertos Como Técnica de Bloqueio de Spam: Transferindo a Responsabilidade para o Remetente**. In Anais da Conferência Ibero-Americana WWW/Internet 2006, Murcia, Espanha, 6 e 7 de Outubro, 2006.

ELIAS, V. G. **Servidor de E-mail - Postfix/Amavisd-**

new/SpamAssassin/ClamAV. 2005. 45 p. Monografia de Pós-Graduação *"Lato Sensu"* em Administração de Redes Linux - Universidade Federal de Lavras, Lavras, MG.

ELLERMANN, F. **Sender Policy Framework – Project Overview**, 2008. Site da Internet. Disponível em: <http://www.openspf.org>. Acesso em: 19 de junho de 2009.

HAMBRIDGE, S.; LUNDE, A. **RFC 2635 - DON'T SPEW - A Set of Guidelines for Mass Unsolicited - Mailings and Postings (spam*)**. Junho, 1999. Disponível em: <http://www.faqs.org/rfcs/rfc2635.html>. Acesso em: 19 de fevereiro de 2009.

HARRIS, E. **The Next Step in the Spam Control War: Greylisting**. 2003. Disponível em: <http://www.greylisting.org/articles/whitepaper.shtm>. Acesso em: 15 de maio de 2009.

HIRD, S. **Technical Solutions for Controlling Spam**, 2002. Australian UNIX User Group (AUUG) Annual Technical Conference. Disponível em: <http://www.lasr.cs.ucla.edu/classes/239_2.spring04/papers/technical_spam.pdf >. Acesso em: 05 de maio de 2009.

JUNIOR, W. T. L. Fatores estruturantes das comunidades virtuais pioneiras nas redes sociais. **LÍBERO - Revista do Programa de Pós-Graduação da Faculdade Cásper Líbero**, ano XI, n. 22. Dezembro, 2008.

KLENSIN, J. **RFC 2821 - Simple Mail Transfer Protocol**. Abril, 2001. Disponível em: <http://www.faqs.org/rfcs/rfc2821.html>. Acesso em: 12 de abril de 2009.

MINDLIN, A. Seems Somebody Is Clicking on That Spam. **The New York Times**. 3 de julho, 2006. Disponível em: <http://www.nytimes.com/2006/07/03/technology/03drill.html? _r=1&ex=1169182800&en=b5bd79833ae87492&ei=5070>. Acesso em: 23 de fevereiro de 2009.

MYERS, J.; MELLON C.; ROSE M. **RFC 1939 - Post Office Protocol - Version 3**. Maio, 1996. Disponível em: <http://www.faqs.org/rfcs/rfc1939.html>. Acesso em: 16 de abril de 2009.

OLIVIERA, L. B. **TrustMail: Um modelo de confiança entre servidores de e-mail**. 2005. 102 p. Dissertação (Mestrado em Informática Aplicada) - Pontifícia Universidade Católica do Paraná, Curitiba, PR.

IDGNOW; PC Advisor/Reino Unido. Brasil é o segundo maior emissor de spams do mundo, diz Sophos. **IDGNOW**, maio, 2009. Disponível em: <http://idgnow.uol.com.br/seguranca/2009/04/30/brasil-e-o-segundo-maior-emissor-de-spams-do-mundo-diz-sophos/>. Acesso em: 04 de maio de 2009.

POSTEL, J. B. **RFC 821 - Simple Mail Transfer Protocol**. Agosto, 1982. Disponível em: <http://www.faqs.org/rfcs/rfc821.html>. Acesso em: 03 de maio de 2009.

RESNICK, P. **RFC 5322 - Internet Message Format**. Outubro, 2008. Disponível em: <http://www.faqs.org/rfcs/rfc2635.html>. Acesso em: 12 de maio de 2009.

SICA, F.C.; UCHÔA, J. Q.; SIMEONE, L. E. **Administração de Redes Linux**. Lavras: Universidade Federal de Lavras, 2003. 92 p. Apostila do Curso de Pós-Graduação "Lato Sensu" em Administração em Redes Linux.

SILVA, W. A. M. **O Problema do Spam e Técnicas de Combate**. 2007. 80 p. Monografia de Pós-Graduação "Lato Sensu" em Segurança em Redes de Computadores - Associação de Ensino Superior de Olinda, Olinda, PE.

TAVIEIRA, D. M. **Mecanismo Anti-Spam Baseado em Autenticação e Reputação**. 2008. 86 p. Dissertação de Mestrado em Engenharia - Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ.

TEIXEIRA, R. C. **O Pesadelo do Spam**. RNP – Rede Nacional de Ensino e Pesquisa. Janeiro, 2001. Disponível em: <http://www.rnp.br/newsgen/0101/spam.html#ng-3>. Acesso em: 14 de abril de 2009.

TEMPLETON, B. **Origin of the Term "Spam" to Mean Net Abuse**. Março, 2003. Disponível em: <http://www.templetons.com/brad/spamterm.html>. Acesso em: 13 de maio de 2009.

TRACElabs. **Spam Statistics - Statistics for Week ending May 24, 2009**.

Maio, 2009. Disponível em: <http://www.marshal8e6.com/TRACE/spam_statistics.asp>. Acesso em: 25 de maio de 2009.

UCHÔA, J. Q. **Configuração Segura do Serviço de E-mail via Postfix**. Palestra ministrada durante o 6º Fórum Internacional de Software Livre – FISL. Junho, 2005. Porto Alegre, RS.

VENEMA, W. Z. **The Postfix Homepage**, 2008. Site da Internet. Disponível em: <http://www.postfix.org>. Acesso em: 30 de maio de 2009.

WONG M.; W. SCHLITT. **Sender Policy Framework (SPF) forvAuthorizing Use of Domains in E-Mail, Version 1**. Abril, 2006. Disponível em: <http://tools.ietf.org/html/rfc4408>. Acesso em: 19 de junho de 2009.

Anexo A – *Log* do servidor de *e-mail*: funcionamento das técnicas anti-*spam*

A) *Greylisting*

Primeira tentativa:

```
Apr 27 11:57:25 bcc postfix/smtpd[28933]: connect from
rumba.ufla.br[200.131.250.17]
Apr 27 11:57:26 bcc postgrey: action=greylist, reason=new,
client_name=rumba.ufla.br, client_address=200.131.250.17,
sender=cqp@ufla.br, recipient=vladimir@bcc.ufla.br
Apr 27 11:57:26 bcc postfix/smtpd[28933]: NOQUEUE: reject: RCPT from
rumba.ufla.br[200.131.250.17]: 450 4.2.0 <vladimir@bcc.ufla.br>: Recipient
address rejected: Greylisted, see
http://postgrey.schweikert.ch/help/bcc.ufla.br.html; from=<cqp@ufla.br>
to=<vladimir@bcc.ufla.br> proto=ESMTP helo=<rumba.ufla.br>
Apr 27 11:57:36 bcc postfix/smtpd[28933]: disconnect from
rumba.ufla.br[200.131.250.17]

(...)
```

Segunda tentativa (realizada antes do término do prazo de espera):

```
Apr 27 11:58:39 bcc postfix/smtpd[28933]: connect from
rumba.ufla.br[200.131.250.17]
Apr 27 11:58:39 bcc postgrey: action=greylist, reason=early-retry (227s
missing), client_name=rumba.ufla.br, client_address=200.131.250.17,
sender=cqp@ufla.br, recipient=vladimir@bcc.ufla.br
Apr 27 11:58:39 bcc postfix/smtpd[28933]: NOQUEUE: reject: RCPT from
rumba.ufla.br[200.131.250.17]: 450 4.2.0 <vladimir@bcc.ufla.br>: Recipient
address rejected: Greylisted, see
http://postgrey.schweikert.ch/help/bcc.ufla.br.html; from=<cqp@ufla.br>
to=<vladimir@bcc.ufla.br> proto=ESMTP helo=<rumba.ufla.br>
Apr 27 11:58:45 bcc postfix/smtpd[28933]: disconnect from
rumba.ufla.br[200.131.250.17]

(...)
```

Próxima tentativa (realizada após o término do prazo de espera). A mensgem é aceita:

```
Apr 27 12:31:51 bcc postfix/smtpd[28988]: connect from
rumba.ufla.br[200.131.250.17]
Apr 27 12:31:51 bcc postgrey: action=pass, reason=triplet found,
```

```
delay=2065, client_name=rumba.ufla.br, client_address=200.131.250.17,
sender=cqp@ufla.br, recipient=vladimir@bcc.ufla.br
Apr 27 12:31:51 bcc postfix/smtpd[28988]: 3CF3514464C:
client=rumba.ufla.br[200.131.250.17]
Apr 27 12:31:51 bcc postfix/cleanup[28981]: 3CF3514464C: message-
id=<1236772271fd5703181cccff7580ae08ebb5aee36e@ufla.br>
Apr 27 12:31:51 bcc postfix/qmgr[2450]: 3CF3514464C: from=<cqp@ufla.br>,
size=1393, nrcpt=1 (queue active)
Apr 27 12:31:52 bcc postfix/pipe[28984]: 3CF3514464C:
to=<vladimir@bcc.ufla.br>, relay=dovecot, delay=2.4,
delays=2.4/0.01/0/0.01, dsn=2.0.0, status=sent (delivered via dovecot
service)
Apr 27 12:31:52 bcc postfix/qmgr[2450]: 3CF3514464C: removed
Apr 27 12:31:52 bcc postfix/smtpd[28988]: disconnect from
rumba.ufla.br[200.131.250.17]
```

B) *Blacklist*

Mensagem rejeitada:

```
May 13 15:35:46 bcc postfix/smtpd[14883]: connect from 118-167-129-
59.dynamic.hinet.net[118.167.129.59]
May 13 15:35:48 bcc postfix/smtpd[14883]: NOQUEUE: reject: RCPT from 118-
167-129-59.dynamic.hinet.net[118.167.129.59]: 554 5.7.1 Service
unavailable; Client host [118.167.129.59] blocked using zen.spamhaus.org;
http://www.spamhaus.org/query/bl?ip=118.167.129.59;
from=<hjoyuo@hotmail.com> to=<vladimir@bcc.ufla.br> proto=SMTP
helo=<200.131.251.13>
May 13 15:35:48 bcc postfix/smtpd[14883]: lost connection after RCPT from
118-167-129-59.dynamic.hinet.net[118.167.129.59]
May 13 15:35:48 bcc postfix/smtpd[14883]: disconnect from 118-167-129-
59.dynamic.hinet.net[118.167.129.59]
```

C) Análise de Corpo e Cabeçalho

Mensagem rejeitada:

```
Apr 29 17:24:09 bcc postfix/smtpd[26174]: connect from rede19-
servidor02.dnsreverso.net[189.84.19.2]
Apr 29 17:24:10 bcc postfix/smtpd[26174]: C53391442E1: client=rede19-
servidor02.dnsreverso.net[189.84.19.2]
Apr 29 17:24:10 bcc postfix/cleanup[26184]: C53391442E1: reject: header
Subject: Energetico VIAGRA NATURAL poderoso para Homens e Mulheres. from
rede19-servidor02.dnsreverso.net[189.84.19.2];
from=<emarketing@activecampaign.com.br> to=<pereira@bcc.ufla.br>
proto=ESMTP helo=<rede19-servidor02.dnsreverso.net>: 5.7.1 No thanks,
we've got plenty.
Apr 29 17:24:10 bcc postfix/smtpd[26174]: disconnect from rede19-
servidor02.dnsreverso.net[189.84.19.2]
```

Anexo B – Regras de configuração da técnica de análise de corpo e cabeçalho

A seguir seguem trechos das regras programadas no MTA para a checagem de corpo e cabeçalho das mensagens. Estes são trechos das configurações, pois o conteúdo integral destes arquivos é muito extenso.

```
####Checagem de anexos potencialmente infectados
/^(.*)name=\"(.*)\.(exe|lnk|dll|shs|vbe|hta|com|vbs|vbe|js|jse|bat|cmd|
vxd|scr|shm|pif|chm)\"$/ DISCARD
/^(.*)name=(.*)\.(exe|lnk|dll|eml|shs|vbe|hta|com|vbs|vbe|js|jse|bat|cmd|
vxd|scr|shm|pif|chm)$/ DISCARD
(…)

#### Rejeita mensagens com codificação não-padrão
/^Subject:.*=\?(GB2312|big5|euc-kr|ks_c_5601-1987|koi8)\?/          REJECT
Unreadable
/^Content-Type:.*charset="?(GB2312|big5|euc-kr|ks_c_5601-1987|koi8|iso-
2022-jp)/ REJECT Unreadable
(…)

#### Checagem de assuntos
/^Subject:.*      / REJECT Space
/^Subject:.*r[  _\.\*\-]+o[  _\.\*\-]+l[  _\.\*\-]+e[  _\.\*\-]+x/  REJECT
Hidden Words
/^Subject:.*p[ _\.\*\-]+o[ _\.\*\-]+r[ _\.\*\-]+n/ REJECT
/^Subject:(.*)sale/          REJECT
/^Subject:(.*)offer/         REJECT
/^Subject:(.*)off/           REJECT
/^Subject:(.*)pharmacy/      REJECT
/^Subject:(.*)pnarmacy/      REJECT
/^Subject:(.*)medicine/      REJECT
/^Subject:(.*)pills/         REJECT
/^Subject:(.*)watches/       REJECT
/^Subject:(.*)discount/      REJECT
/^Subject:(.*)illness/       REJECT
/^Subject:(.*)sex/           REJECT
/^Subject:(.*)hot/           REJECT
/^Subject:(.*)sexy/          REJECT
/^Subject:(.*)pron/          REJECT
/^Subject:(.*)bitch/         REJECT X-Rated Subject Line
/^Subject:(.*)bodies/        REJECT X-Rated Subject Line
/^Subject:(.*)breast/        REJECT X-Rated Subject Line
/^Subject:(.*)fuck/          REJECT X-Rated Subject Line
```

```
/^Subject:(.*)galore/         REJECT X-Rated Subject Line
/^Subject:(.*)porn/           REJECT X-Rated Subject Line
/^Subject:(.*)slut/           REJECT X-Rated Subject Line
/^Subject:(.*)HARDCORE/       REJECT X-Rated Subject Line
/^Subject:(.*)teen/           REJECT X-Rated Subject Line
/^Subject:(.*)viagra/         REJECT No thanks, we've got plenty.
/^Subject:(.*)ejaculation/    REJECT No thanks, we've got plenty.
/^Subject:(.*)viaagra/        REJECT No thanks, we've got plenty.
/^Subject:(.*)viiagra/        REJECT No thanks, we've got plenty.
(…)

#### Ignorar notificações de anti-virus
/^Subject:.*Anti-Virus Notification/ REJECT Virus Notification
/^Subject:.*due to virus/             REJECT Virus Notification
/^Subject:.*email contains VIRUS/     REJECT Virus Notification
/^Subject:.*InterScanMSS/             REJECT Virus Notification
/^Subject:.*ScanMail for Lotus/       REJECT Virus Notification
/^Subject:.*Symantec AntiVirus/       REJECT Virus Notification
/^Subject:.*Virus   Detected   by   Network   Associates/   REJECT   Virus
Notification
/^subject:.*virus found/              REJECT Virus Notification
/^subject:.*Virus Infection Alert/    REJECT Virus Notification
(…)
```