PROJETO DE REDES
www.projetoderedes.com.br

AESO
FACULDADES INTEGRADAS BARROS MELO

O PROBLEMA DO SPAM E TÉCNICAS DE COMBATE

WAGNER ALBUQUERQUE MENEZES SILVA

WAGNER ALBUQUERQUE MENEZES SILVA

O PROBLEMA DO SPAM E TÉCNICAS DE COMBATE

Monografia apresentada ao Curso de Pós-Graduação em Segurança em Redes de Computadores, da Associação de Ensino Superior de Olinda, como requisito à obtenção do título de Especialista.

Orientador: Prof. Msc. Rodrigo Assad

WAGNER ALBUQUERQUE MENEZES SILVA

O PROBLEMA DO SPAM E TÉCNICAS DE COMBATE

Monografia apresentada ao Curso de Pós-Graduação em Segurança em Redes de Computadores, da Associação de Ensino Superior de Olinda, como requisito à obtenção do título de Especialista.

COMISSÃO EXAMINADORA

_____
Prof. Msc. Rodrigo Assad
Associação de Ensino Superior de Olinda

_____
Prof.

_____
Prof.

Olinda, _____ de novembro de 2007.

Dedico este trabaho aos meus pais, esposa, irmãos e amigos, que me transformaram em quem sou hoje.

AGRADECIMENTOS

Aos meus pais, Fernando e Aidé, que durante toda minha vida me proporcionaram a maior das heranças: a educação. Sem a sabedoria e carinho deles, este trabalho não teria sido formado.

A minha esposa, Graça, que está sempre ao meu lado, me fornecendo o amor necessário para continuar minha jornada. Seu incentivo para iniciar a pós-graduação foi essencial para a continuação de minha formação acadêmica. Sua ajuda nas discussões e revisões da monografia foi de fundamental importância para a conclusão do trabalho.

A todos meus amigos, em especial Uriel Kadmo, Rafael Arcúrio, Hedwio Carvalho e Arnaldo Leite que estão entre os principais responsáveis pelo meu crescimento profissional nas áreas de administração de serviços de redes e segurança da informação.

A todos os professores da AESO, em especial ao mestre Rodrigo Assad, que com seus conhecimentos acadêmicos e profissionais tornaram o curso de Especialização em Segurança em Redes de Computadores uma referência para os profissionais da área. Eles conseguiram fazer com que um incrédulo em cursos de Especialização Lato-Sensu conseguisse rever seus conceitos e aceitar que alguns desses cursos não são meros revisores de cursos de graduação.

A todos os funcionários da AESO, que, conjuntamente com os alunos e professores, sacrificaram suas sextas-feiras e sábados para oferecer o suporte necessário à realização do curso.

RESUMO

A Internet transformou a distância em um simples detalhe e promoveu uma revolução na comunicação. O *e-mail* passou de um simples coadjuvante na nova tecnologia de comutação de pacotes para o meio de comunicação mais utilizado na rede mundial de computadores. Como conseqüência de sua popularização, o *e-mail* deu origem ao *spam*. Os problemas causados pelo *spam* são inúmeros e o seu combate deverá durar por vários anos. As técnicas *anti-spam* tentam minimizar a chegada do *spam* às caixas de mensagens dos usuários. O estudo dessas técnicas permite a escolha de quais delas são as mais adequadas para cada ambiente.

ABSTRACT

The Internet has changed the distance into a simple detail and promoted a revolution in the communication. The *e-mail* stepped by a simple coadjuvant on new packet switching technology to the most used communication mean in the worldwide computer network. As consequence of its popularization, the *e-mail* originated the *spam*. The problems caused by spam are innumerous and its fight will remain for long years. The anti-spam techniques try to minimize the arrive of spam to the user's mailbox. The study of these techniques allow the choice among the more suitable ones for each environment.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA - Advanced Research Projects Agency

ARPANET - Advanced Research Projects Agency Network

CGI.br – Comitê Gestor da Internet no Brasil

CETIC.br – Centro de Estudos sobre as Tecnologias da Informação e das Comunicações no Brasil

CERT.br – Centro de Estudos, Respostas e Tratamento de Incidentes no Brasil

DEC – Digital Equipment Corporation

DHA – *Directory Harvest Attack*

DKIM – *DomainKeys Identified Mail*

DNS - Domain Name System

DoD – Department of Defense

EUA – Estados Unidos da América

FBI – Federal Bureau of Investigations

HTML – Hyper Text Markup Language

IANA - Internet Assigned Numbers Authority

IDC – International Data Corporation

IP – Internet Protocol

MILNET – Military Network

MIME - Multipurpose Internet Mail Extensions

PGP – Pretty Good Privacy

PDF – Portable Document Format

RFC - Request For Comments

ROSKO – Register of Known Spam Operations

SPF – *Sender Policy Framework*

TCP – Transmission Control Protocol

URSS – União das Repúblicas Socialistas Soviéticas

RNP – Rede Nacional de Pesquisa

SMTP - Simple Mail Transfer Protocol

S/MIME - Secure / Multipurpose Internet Mail Extensions

UCE - Unsolicited Comercial E-mail

USENET – User Network

US-ASCII – United States American Standard Code for Information Interchange

VoIP – Voice over Internet Protocol

SUMÁRIO

1 INTRODUÇÃO

1.1 Visão Geral

Em 7 de fevereiro de 1958, a diretiva 5105.15 do Departamento de Defesa dos Estados Unidos da América (DoD) criou a Agência de Projetos em Pesquisa Avançada, *Advanced Research Project Agency Network* (ARPA), que tinha a responsabilidade de dar a direção das pesquisas e desenvolvimentos encabeçados pelo DoD.[1]

Por volta de 1962, J.C.R. Licklider, um integrante da ARPA começou a discutir sobre os conceitos de uma "Rede Galática", uma rede de escala global que interconectaria um conjunto de computadores, fazendo com que as pessoas trocassem informações, estando elas em qualquer parte do mundo.

A ARPA foi a agência pioneira no trabalho com comutação de pacotes, tecnologia até então pouco pesquisada e que pretendia ser a substituta da comutação de circuitos. Apesar dos estudos da ARPA, em uma tecnologia de interconexão de redes comutadas por pacotes, ter iniciado formalmente no início da década de 1970, essa tecnologia e seus protocolos tomaram forma em meados de 1979.

A *Advanced Research Project Agency Network* (ARPANET), a rede comutada por pacotes da ARPA, foi desmembrada em duas por volta de 1980, a *Military Network* (MILNET), rede de uso exclusivo militar, e a própria ARPANET, que agregou projetos de pesquisas e interligações com universidades americanas. Mesmo desmembradas, as duas redes utilizavam um novo conjunto de protocolos denominados TCP/IP. Este nome é devido a seus principais protocolos, o *Transmission Control Protocol* (TCP)[2] e o *Internet Protocol* (IP)[3]. Ao conjunto dessas redes que estavam interconectadas foi denominado Internet.

O grande benefício vislumbrado pela ARPA para essas novas redes comutadas por pacotes e utilizando a pilha de protocolos TCP/IP foi em relação a disponibilidade de comunicação. Mesmo que alguns pontos de comunicação se tornassem inoperantes, leiam-se atacados, uma vez que os Estados Unidos da

---

[1] Maiores informações sobre a criação da ARPA podem ser obtidas em http://www.darpa.mil/body/arpa_darpa.html

[2] A descrição do protocolo TCP pode ser obtida em http://www.ietf.org/rfc/rfc0793.txt

[3] A descrição do protocolo IP pode ser obtida em http://www.ietf.org/rfc/rfc791.txt

América (EUA) e a extinta União das Repúblicas Socialistas Soviéticas (URSS) estavam em plena guerra fria, as comunicações entre os outros pontos permanecia em funcionamento.

O grande impulsionador da interconexão das redes já existentes no Brasil foi a Rede Nacional de Pesquisa (RNP)[1], que tornou-se o *backbone* nacional de interconexão de redes no país. A Internet começou a ser utilizada de fato pelos usuários domésticos no Brasil por volta de 1995, quando a RNP decidiu abrir seu *backbone* para os provedores de acesso comerciais.

Desde o seu surgimento até os dias atuais, a Internet causou uma verdadeira revolução nos hábitos e costumes em todo o mundo. Ela tornou-se um dos maiores veículos de comunicação, fazendo com que as relações econômicas, sociais e pessoais ganhassem nova forma, acessíveis para uma grande quantidade de pessoas.

A Internet trouxe os seguintes benefícios: reduziu as distâncias geográficas e aumentou a rapidez com que as pessoas trocam informações, podendo, atualmente, pessoas em pontos extremos do planeta estarem se comunicando, trocando documentos, realizando video-conferências em tempo real.

Porém, assim como a maioria das tecnologias desenvolvidas pelo ser humano, a Internet também é utilizada para fins negativos. O *spam* é uma das formas de se utilizar negativamente a Internet. *Spam* é definido pelo Comitê Gestor da Internet no Brasil (CGI.br)[2] como "*e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas". Quando essas mensagens têm conteúdo exclusivamente comercial, as mesmas são denominadas *Unsolicited Comercial E-mail* (UCE).

O primeiro *spam* enviado por *e-mail* em uma internet é datado de 1978. Einar Stefferud, um funcionário da empresa *Digital Equipment Corporation* (DEC) anunciou a nova máquina DEC-20 enviando um convite a todos os integrantes da ARPANET que moravam na costa oeste para uma recepção na California. Apesar desta mensagem ter sido o primeiro *spam* via *e-mail*, a mesma não foi a originária do termo.

---

[1] A RNP foi criada em 1989 pelo Ministério da Ciência e Tecnologia com o objetivo de construir uma infra-estrutura de rede Internet nacional para a comunidade acadêmica. Maiores informações sobre a RNP podem ser obtidas em http://www.rnp.br

[2] O CGI.br foi criado pela Portaria Interministerial no 147 em 1995 para coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Maiores informações em http://www.cgi.br/

No início de 1994, Laurence Canter e Martha Siegel, advogados da cidade de *Phoenix*, postaram uma mensagem na *User Network* (USENET), o maior sistema de conferência *online*, anunciando seus serviços de ajuda na obtenção do tão desejado *Green Card*. Apesar da postagem ter irritado os usuários da USENET, o pior ainda estava por vir. Siegel e Canter contrataram um programador que desenvolveu um *script* que postou, em 12 de abril de 1994, seus anúncios em todos os grupos do USENET. O Anexo A apresenta algumas das mensagens enviadas por Laurence e Martha na USENET.

Durante as discussões sobre a violação das regras de bom uso da USENET, ocorreram várias citações à palavra *spam*. A palavra tem como referência uma cena do grupo de TV inglês *Monty Python*, em que no seu programa *Monty Python's Flying Circus*, um restaurante serve todas as suas comidas com muito *SPAM*® (***SP****iced h****AM***), um condimentado de presunto fabricado pela empresa *Hormel Foods*. Durante o programa, um grupo de vikings recita diversas vezes a frase "*Spam, spam, spam, spam, spam, spam, spam, spam, lovely spam! Wonderful spam!*". A associação com a palavra *SPAM* deriva do fato de que algo repetido diversas vezes torna-se irritante.

Apesar de, em uma análise superficial, ser considerado um mero aborrecimento, o *spam* é, de fato, um problema que impacta principalmente nas atividades profissionais e econômicas da sociedade.

Nas atividades profissionais, o principal problema do *spam* é a diminuição da produtividade dos funcionários, que desperdiçam seu tempo abrindo e analisando *e-mails* que são apenas *spam*.

Os impactos econômicos gerados pelo *spam* podem ser constatados em diversos aspectos. A empresa de consultoria *International Data Corporation* (IDC) projetou, em sua recente pesquisa, que o *spam* chegue a 40 bilhões de mensagens no ano de 2007, gerando um total de seis a sete mensagens para cada ser humano no mundo, número superior aos de *e-mails* legítimos trocados durante o mesmo período (IDG NOW!, 2007). O IDC estima também que o volume total de tráfego gerado pelo *spam* será de aproximadamente cinco hexabytes. Esses números significam que a infra-estrutura de rede da Internet está sendo utilizada para o tráfego oriundo do *spam*, o que pode ser traduzido como perda financeira dos investimentos em infra-estrutura para a Internet.

Além do prejuízo derivado do consumo de largura de banda utilizada, o *spam* atualmente proporciona um dos mais efetivos meios utilizados por quadrilhas organizadas de estelionatários para realizar o famoso ataque de *phishing scam*.

Phishing scam é uma técnica de Engenharia Social utilizada para adquirir informações sensíveis como números de cartões de crédito, senhas e dados bancários ou para induzir as pessoas a baixar e executar arquivos que permitam o furto futuro de informações ou o acesso não autorizado a sistemas das vítimas. Através do *spam*, o estelionatário envia *e-mails* para milhões de pessoas em um curtíssimo intervalo de tempo a um custo quase zero. Devido à grande quantidade de pessoas que recebem este tipo de *spam*, a chance de sucesso do ataque é muito grande.

Com uma quantidade cada vez maior de *spam* circulando pela Internet, surgiu a necessidade de criação de técnicas que fossem capazes de detectar se uma mensagem é ou não *spam* e assim impedir, que a mensagem chegue à caixa de mensagens do usuário.

1.2 Objetivos Gerais

Com a crescente popularização do acesso aos computadores e com o decrescente custo de acesso, a Internet vem se tornando um item essencial para a vida das pessoas. O que antes era luxo, hoje se torna uma necessidade. A democratização do acesso à Internet é um dos projetos do atual governo brasileiro. O ingresso na rede mundial de computadores tornou-se item obrigatório para as empresas que querem e as que já se firmaram e almejam continuar no mercado. Os governos utilizam a Internet como um dos meios de prestação de contas com a população, garantindo assim uma maior transparência na administração pública.

A conseqüência básica do aumento do número de acessos à Internet é a utilização do *e-mail* como o principal meio de comunicação em utilização na rede. A quantidade de provedores de *e-mail* e a facilidade na utilização de programas clientes para o envio e recebimento de mensagens ajudaram a popularizá-lo. As organizações contam cada vez mais com a utilização desta técnica para a troca de informações com seus clientes e até mesmo para o envio e recebimento de informações sigilosas.

Este trabalho tem vários objetivos gerais, iniciando pela origem do meio de comunicação mais utilizado na Internet, o *e-mail*. O protocolo de aplicação *Simple Mail Transfer Protocol* também possui atenção especial, uma vez que ele é o protocolo facilitador da transmissão de mensagens eletrônicas. Serão apresentados a estrutura básica do SMTP e os procedimentos operacionais, com alguns comandos mais utilizados, que são definidos pelo documento que especifica o protocolo. Outro objetivo é mostrar algumas questões de segurança do protocolo, uma vez que devido a sua fragilidade ele pode ser explorado facilmente para enviar *spam*.

Além dos objetivos gerais já citados, incluem-se a apresentação das definições de *spam*, quais são os seus principais tipos, suas mutações durante sua expansão pela Internet, os problemas surgidos pela disseminação do *spam* e algumas estatísticas que apresentam os números gigantescos dessa praga virtual.

1.3 Objetivos Específicos

O *spam* apareceu como um mero aborrecimento para os destinatários desse tipo de mensagem eletrônica. Com o crescimento do número de usuários e serviços oferecidos pela rede mundial de computadores, o *spam* começou a ameaçar os lucros das organizações que se ligavam à Internet. Além disso, com o advento dos sites bancários, com opções de movimentação bancária, pagamento de contas, entre outros, ele tornou-se o principal meio para a execução do tipo penal definido no artigo 171 do Código Penal Brasileiro, ou seja, estelionato.

Todos sabem que, para acabar com o *spam*, deve-se simplesmente acabar com o seu originador. Apesar de essa solução ser conhecida, ela é muito difícil de ser implementada. Já existem mapeamentos de organizações nacionais e internacionais especializadas que são contratadas para o envio de *spam* em massa. O problema que ocorre é que os países que concentram os maiores difusores de *spam* são aqueles que não possuem ou possuem uma fraca legislação de combate a esta prática. Se não há a definição do tipo penal para os disseminadores de *spam*, os *spammers*, não há como esses países combatê-los. Com isso, o Estado repassa para a sociedade civil o ônus de tentar minimizar a chegada dessas mensagens eletrônicas nas caixas de mensagens dos usuários da Internet.

Como objetivos específicos, o trabalho apresenta e difunde algumas das principais técnicas de filtragem de *spams*. São apresentadas técnicas de listas negras de tempo-real, pesos e regras, listas cinzas, *Sender Police Framework* e *Domainkeys Identified Mail*.

A apresentação dessas técnicas deve fornecer subsídio para o usuário de *e-mail* ou administrador de rede avaliar as diversas soluções *anti-spam* e entender o trabalho realizado por elas.

1.4 Motivação

Trabalhar como administrador de redes de computadores é algo desafiador. A cada momento surgem situações adversas às quais o profissional nunca enfrentou. No exercício da função de administrador de redes, a análise da problemática do *spam*, na maioria das vezes, é algo mais simples, pois exige apenas que o administrador faça os ajustes necessários na solução *anti-spam* da corporação para que os usuários recebam uma quantidade ínfima de *spam*. A eficiência da ferramenta é medida pelo administrador através do parâmetro da quantidade deste tipo de mensagem que chega às caixas de *e-mail* dos usuários finais.

Algo mais desafiador que trabalhar apenas como administrador de redes é agregar esta função com a de analista de segurança da informação. Como profissional de segurança da informação, a análise do *spam* vai muito além de constatar o mero aborrecimento do usuário em relação ao *spam* que chegou à caixa de *e-mail*. É necessário verificar quais são os tipos principais de *spam* que ultrapassam as ferramentas de bloqueio, analisar se eles estão carregando algum tipo de programa malicioso que afete a segurança da informação da organização, estudar quais são as principais técnicas *anti-spam* que existem na atualidade para tentar reduzir não o aborrecimento dos usuários e sim as ameaças à segurança da informação na organização.

O estudo do *spam*, incluindo sua origem, mutações e problemáticas, gera uma maior motivação para o estudo das técnicas utilizadas pelas ferramentas *anti-spam*. O conhecimento de quais técnicas são utilizadas por quais ferramentas oferece ao profissional de segurança uma maior certeza de escolher a solução que mais se adeqüe para o combate ao *spam* na organização em que exerce suas funções.

2 O E-MAIL

2.1 Origem do E-Mail

O *e-mail* na Internet surgiu quando, em 1972 Ray Tomlinson, um contratado da ARPANET para o desenvolvimento do sistema operacional TENEX, resolveu modificar o programa de mensagem SNDMSG. Como o SNDMSG enviava mensagens apenas para os usuários conectados ao mesmo computador servidor de terminal, Tomlinson o adaptou e o transformou no CPYNET, um programa capaz de realizar cópias de arquivos através da rede.

Durante o desenvolvimento do CPYNET, Tomlinson resolveu criar uma sintaxe para o endereçamento das mensagens. Ele resolveu utilizar o símbolo @ para combinar o *login* do usuário ao computador de destino, formando o até hoje utilizado endereçamento de e-mail "usuário@host".

Em 1977, a ARPA decidiu formar um subcomitê do *Computer-Aided Human Communication* (CAHCOM) para "promulgar um padrão para o formato dos cabeçalhos das mensagens de texto (mail) da Rede ARPA" (CROCKER, 1977, tradução nossa). O subcomitê formado por David Crocker, John Vittal, Kenneth Progran e Austin Henderson, conseguiu reunir vários formatos de mensagens eletrônicas e consolidá-las em uma única e coerente especificação, resultando na *Request For Comments* (RFC) 733: *Standard for the Format of ARPA Network Text Messages*.[1]

Durante o ano de 1982 David Crocker revisou as especificações da RFC 733, o que resultou na RFC 822, *Standard for the Format of ARPA Internet Text Messages*.[2] A revisão surgiu da necessidade de adaptação da RFC 733 ao imenso crescimento de tamanho e complexidade da ARPANET. Os principais pontos da revisão foram a retirada de alguns atributos que não foram amplamente aceitos, um esquema de endereçamento diferente para se adaptar ao envio de *e-mails* entre redes interconectadas e a introdução ao conceito de re-transmissão.

Em paralelo ao desenvolvimento da RFC 733, Jonathan Bruce Postel, diretor do *Internet Assigned Numbers Authority* (IANA), trabalhou e desenvolveu um

[1] A RFC 733 pode ser encontrada em http://www.ietf.org/rfc/rfc733.txt
[2] A RFC 822 pode ser encontrada em http://www.ietf.org/rfc/rfc822.txt

protocolo confiável e eficiente para a transmissão de *e-mail*. O trabalho de Jonathan foi publicado como a RFC 821, *Simple Mail Transfer Protocol*, ou SMTP.

Atualmente, as mensagens e a infra-estrutura de suporte de transmissão de *e-mail* utilizam basicamente as especificações dos protocolos descritos nas RFCs 2822, *Internet Message Format*[1], e 2821, *Simple Mail Transfer Protocol*[2], que são revisões das RFCs 822 e 821 respectivamente.

2.2 Simple Mail Transfer Protocol

O protocolo SMTP faz parte do conjunto de protocolos da camada de aplicação da arquitetura de redes TCP/IP. O objetivo do SMTP é a transferência confiável e eficiente de mensagens eletrônicas.

Conforme sua especificação, o SMTP é "independente de subsistemas de transmissão particulares e requer apenas um canal de transmissão de dados confiável e ordenado" (KLENSIN, 2001, tradução nossa). Uma importante característica do SMTP é a possibilidade de transmissão de *e-mail* para destinos em uma mesma rede ou em redes diferentes.

2.2.1 A Estrutura Básica do SMTP

O modelo de transmissão de *e-mail* adotado pelo SMTP pode ser visto de acordo com a Figura 1:

Figura 1. Modelo de transmissão do SMTP

[1] A RFC 2822 pode ser encontrada em http://www.ietf.org/rfc/rfc2822.txt
[2] A RFC 2821 pode ser encontrada em http://www.ietf.org/rfc/rfc2821.txt

O mecanismo básico de transmissão do SMTP baseia-se no modelo cliente-servidor. Quando um cliente deseja transmitir um *e-mail*, ele 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 na porta 25. Uma vez estabelecida a conexão, o cliente transmite a mensagem para o servidor ou reporta para o usuário alguma falha de envio.

Não faz parte do protocolo SMTP determinar se a mensagem a ser entregue é destinada ao servidor local ou a algum servidor remoto de SMTP. O programa cliente SMTP é que é responsável por pesquisar o servidor de *e-mail* remoto que implementa o SMTP, geralmente, em internet TCP/IP, resolvendo o nome do domínio de destino através de consulta ao registro ***M**ail e**X**changer* do servidor Domain Name System (DNS) responsável pelo domínio em questão.

É importante destacar que a RFC 2821 preconiza que:

> Um servidor SMTP pode ser tanto o destino final ou um *"relay"* intermediário (isto é, ele pode assumir o papel de um cliente SMTP depois de receber a mensagem) ou *"gateway"* (isto é, ele pode transportar a mensagem depois utilizando um protocolo diferente do SMTP). Comandos SMTP são gerados pelo cliente SMTP e enviados ao servidor SMTP. Respostas SMTP são enviadas do servidor SMTP para o cliente SMTP em resposta aos comandos. (KLENSIN, 2001, tradução nossa).

O que a RFC 2821 quis enfatizar é que a conexão SMTP pode ser estabelecida entre o cliente original SMTP e o servidor SMTP final ou entre uma seqüência de servidores intermediários. Em ambas as situações a RFC 2821 impõe:

> [...] uma transferência formal de responsabilidade pela entrega da mensagem ocorre: o protocolo exige que um servidor aceite a responsabilidade de tanto entregar a mensagem ou reportar propriamente a falha que ocorreu. (KLENSIN, 2001, tradução nossa).

Após o estabelecimento da conexão da camada de transporte, o cliente SMTP inicia com o servidor a transação de transferência. Essa transação consiste em uma seqüência de comandos enviados pelo cliente que especificam a origem e o destinatário da mensagem. Após esta seqüência de comandos, o conteúdo propriamente dito é enviado.

Cada comando enviado pelo cliente SMTP é respondido pelo servidor com um código. Cada código pode indicar que o comando recebido foi aceito, que comandos adicionais são necessários, ou que erros temporários ou definitivos ocorreram. Após o envio da mensagem, o cliente SMTP pode solicitar o fechamento da conexão ou pode iniciar o envio de uma nova mensagem.

2.2.2 Os Procedimentos do SMTP

O protocolo SMTP faz o transporte de objetos *mail*. Estes objetos transportados são constituídos de um envelope e um conteúdo.

O envelope SMTP é uma seqüência de comandos SMTP enviados pelo cliente e contêm informações como o remetente, destinatário e algumas extensões do protocolo.

O conteúdo de um objeto *mail* é enviado no comando SMTP DATA e também possui uma divisão de partes: cabeçalho e corpo. O conteúdo de um objeto *mail* é formatado de acordo com as especificações da RFC 2822. De acordo (RESNICK, 2001), os campos do cabeçalho são formados por linhas compostas de um nome de campo, seguido por um dois pontos (":"), seguido pelo corpo do campo e terminado pelos caracteres de retorno de carro e alimentação de linha. O corpo é de natureza textual, constituído de caracteres United States-American Standard Code for Information Interchange (*US-ASCII*). Ele também pode ser constituído de extensões do tipo Multipurpose Internet Mail Extensions (*MIME*)[1], que definem algoritmos para representar os conteúdos dos campos em formato diferente do *US-ASCII*, embora os mesmos ainda sejam representados como tal.

Uma sessão SMTP é iniciada após o estabelecimento de uma conexão de camada de transporte. Após o estabelecimento dessa conexão, o servidor responde com um código de abertura (220).

A RFC 8221 especifica que as implementações SMTP podem incluir, após a mensagem de código de abertura, informações que identifiquem o software SMTP. Dentre outras, geralmente são incluídas informações sobre o fabricante e a versão do software SMTP. É prática comum de alguns administradores de rede, remover as informações de fabricante e versão do software SMTP para evitar que essas informações forneçam subsídios importantes para atacantes explorarem vulnerabilidades conhecidas do software servidor. Em substituição da tupla fabricante/versão, geralmente é fornecido informação sobre o *e-mail* do administrador do sistema.

O protocolo SMTP especifica que um servidor pode rejeitar uma sessão mesmo aceitando uma conexão inicial. Para isto, em vez do servidor retornar o

[1] A especificação completa do MIME é descrita em cinco documentos. Os mesmos podem ser encontrados em: http://www.ietf.org/rfc/rfc2045.txt, http://www.ietf.org/rfc/rfc2046.txt http://www.ietf.org/rfc/rfc2047.txt http://www.ietf.org/rfc/rfc2048.txt e http://www.ietf.org/rfc/rfc2049.txt

código SMTP de sucesso (220), o mesmo retorna para o cliente o código “554”. Apesar de rejeitar a conexão, o servidor deverá esperar que o cliente envie o comando QUIT, e deverá enviar o código 503 (*bad sequence of commands*) caso o cliente insista em tentar enviar um *e-mail*.

Após a conexão inicial e o retorno do código de sucesso pelo servidor, o cliente deve enviar o comando EHLO (KLENSIN, 2001). O comando EHLO informa para o servidor que o cliente SMTP tem suporte às extensões definidas na RFC 2821 e com isto está solicitando que o servidor informe quais são as extensões suportadas por ele. É importante frisar que:

> Sistemas SMTP antigos que são incapazes de suportar o serviço de extensões e clientes atuais que não requerem serviços de extensões na sessão de *e-mail* sendo iniciada, pode utilizar HELO em vez de EHLO. Servidores NÃO DEVEM retornar a resposta extendida do tipo EHLO em resposta a um comando HELO. Para uma tentativa particular de conexão, se o servidor retornar um “comando não reconhecido” como resposta para um EHLO, o cliente deve ser capaz de voltar e enviar um HELO. (KLENSIN, 2001, tradução nossa).

Após o comando EHLO, existem três passos para completar uma transação básica SMTP. Estes três passos são executados em seqüência pelos comandos MAIL, RCPT e DATA.

A sintaxe do comando MAIL é: MAIL FROM: **<remetente>** [**extensões-mail**]

Este comando informa para o servidor que um envio de *e-mail* está iniciando e que ele deve reiniciar suas tabelas de estado e *buffers*. O parâmetro obrigatório <remetente> indica o *e-mail* do originador da mensagem, *e-mail* este que deve ser utilizado para reportar eventuais erros na transação. O parâmetro opcional **extensões-mail** é utilizado para informar ao servidor algumas das extensões suportadas pelo cliente de acordo com (KLENSIN, 2001). Caso o comando MAIL seja aceito, o servidor retornará o código “250 OK”.

Para o comando RCPT, a sintaxe é: RCPT TO: **<destinatário>** [**extensões-rcpt**]

O parâmetro obrigatório <destinatário> inclui o endereço de *e-mail* do destinatário. O parâmetro opcional **extensões-rcpt** é utilizado para informar ao servidor algumas das extensões suportadas pelo cliente de acordo com (KLENSIN, 2001). Se o comando RCPT for aceito, o servidor retornará o código “250 OK”. Se o endereço do destinatário não for reconhecido, o servidor SMTP retornará o comando “550”, geralmente incluindo a cadeia de caracteres “*no such user* – “, acrescentando

em seguida o endereço do destinatário não reconhecido. O comando RCPT pode aparecer qualquer número de vezes.

O último comando para o procedimento de transação SMTP é o DATA. A sintaxe do comando DATA é: DATA <CRLF>, onde <CRLF> são os caracteres ASCII para retorno de carro e alimentação de linha. Se o comando for aceito pelo servidor, o mesmo retornará o código “354” e considerará todas as linhas sucessoras até, mas não incluindo, o indicador de fim de *e-mail*, como a mensagem de texto. O indicador de fim de *e-mail* é representado pelo envio de uma linha contendo apenas o sinal “.” (ponto).

O indicador de fim de *e-mail* também é utilizado para informar o fim da transação de envio de *e-mail*, fazendo com que o servidor possa armazenar a mensagem recebida na caixa de mensagens do destinatário. Se o comando for aceito, o servidor retornará o comando “250 OK”.

A figura 2 representa os passos de uma transação ocorrida para o envio de *e-mail* através do protocolo SMTP.

Figura 2. Transação de envio de *e-mail*

Apesar da maioria das transações SMTP serem feitas atualmente conforme os passos descritos anteriormente, o protocolo oferece mais comandos a serem utilizados.[1] Outros dois comandos merecem destaque são o VRFY e EXPN.

[1] A totalidade de comandos SMTP pode ser encontrada em www.ietf.org/rfc/rfc2821.txt

O comando VRFY solicita ao servidor STMP que está recebendo o *e-mail* que ele confirme se o argumento utilizado no comando realmente identifica uma caixa de *e-mail* ou usuário presente no sistema. A sintaxe do comando é: "VRFY <**string**> CRLF".

Já o EXPN solicita ao servidor SMTP de destino que confirme se o argumento utilizado no comando identifica uma *mailing list*[1], e se for, retorne os membros da mesma. A sintaxe do comando é: "EXPN <**string>** CRLF".

2.2.3 Considerações de Segurança no SMTP

Apesar de ser um dos protocolos mais utilizados na Internet, o SMTP, quando desenvolvido em 1982, e revisado em 2001, não tinha como requisito a segurança das transações no envio de mensagens eletrônicas.

O protocolo foi especificado para se obter o máximo de facilidade na transmissão das mensagens. Porém, em segurança da informação, um fato é certo: quanto maior a facilidade e/ou funcionalidade, menor é a segurança. (KLENSIN, 2001) informa que:

> O *e-mail* SMTP é inerentemente inseguro uma vez que é possível para até mesmo usuários casuais negociarem diretamente com os servidores SMTP finais ou *relays* e criar mensagens que irão enganar um destinatário ingênuo acreditando que elas vieram de outra pessoa. Construir uma mensagem dessas em que o comportamento "enganador" não pode ser detectado por um especialista é um pouco mais difícil, mas não suficientemente dissuador para alguém que é determinado e possui conhecimento. (KLENSIN, 2001, tradução nossa).

O resultado é que quanto maior é o conhecimento das pessoas sobre a Internet, maior é o conhecimento sobre a fragilidade do protocolo SMTP, que por sua vez não provê em suas origens autenticação ou verificação de integridade. A segurança requerida de autenticidade e integridade são delegadas para outros protocolos de aplicação, como o Pretty Good Privacy (PGP)[2] ou Secure/Multipurpose Internet Mail Extensions (S/MIME)[3].

---

[1] Mailing list é um endereço utilizado por uma pessoa ou organização para enviar e-mail para vários destinatários. Uma organização pode ter vários endereços de mailing list para enviar e-mails para vários destinatários

[2] Aplicação e protocolo criado por Phil Zimmermann que pode prover serviços de confidencialidade e autenticação que podem ser utilizados para e-mails e aplicações de armazenamento de arquivos. Atualmente é definido pela RFC 2440 que pode ser consultada em http://www.ietf.org/rfc/rfc2440.txt

[3] S/MIME é um padrão público para criptografia e assinatura digital de e-mail. A RFC 2633 descreve o protocolo e pode ser encontrada em http://www.ietf.org/rfc/rfc2633.txt

Considerações adicionais devem ser feitas sobre os comandos VRFY e EXPN. A utilização desses comandos permite a um atacante validar endereços de *e-mail* válidos na organização. Nos últimos anos, as mailing lists se tornaram os alvos principais dos *spammers*. Eles utilizam o comando EXPN para fazer um *harvest* (coleta) dos endereços integrantes destas listas, aumentando consideravelmente seus bancos de dados de *e-mails* válidos. Apesar de a RFC recomendar a implementação desses comandos, ela faz uma ressalva sobre eles, informando que os administradores de sistemas devem avaliar cuidadosamente a habilitação dos mesmos.

3 O SPAM

3.1 Definições

O desejo de todo usuário é que sua organização ou provedor de *e-mail* possua uma boa ferramenta *anti-spam*, isto é, uma que, ou coloque em quarentena todas as mensagens de *spam*, e nem as envie para sua caixa de *e-mail*, ou que as marque como *spam* e envie para uma pasta especial da caixa de *e-mail*.

Para fazer a avaliação se uma ferramenta *anti-spam* é boa, primeiro deve-se definir o que é *spam*. As concordâncias e discordâncias das definições giram em torno das mensagens serem não-solicitadas, cunho comercial e automatizadas. De fato, o único consenso existente, gerado pelas definições, é que o *spam* tem o poder de aborrecer o usuário. A seguir são apresentadas algumas definições, incluindo a definição adotada neste trabalho.

O instituto de pesquisa internacional IDC divide o tráfego de *e-mail* em três categorias, sendo a de *spam* definida como:

> Spam é uma "grande quantidade de *e-mail* não solicitado" enviado tanto por marketólogos legítimos oferecendo produtos comerciais e serviços quanto por empresas com menos reputação e indivíduos oferecendo produtos ilícitos, ofensivos e até mesmo não existentes e serviços ou utilizando *e-mail* para distribuir vírus. "Grande quantidade de *e-mail*" é automatizada, a entrega massiva de *e-mail* tende a ter baixo custo e taxas de resposta relativas a campanhas de marketing tradicionais de mala direta e telefone. (LEVITT, 2004, tradução nossa)

Já (TEIXEIRA, 2001) apresenta a seguinte definição:

> [...] *spam* é considerado um abuso e se refere ao envio de um grande volume de mensagens não solicitadas, ou seja, o envio de mensagens indiscriminadamente a vários usuários, sem que estes tenham requisitado tal informação. 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)

Em seu excepcional artigo, (GRAHAM, 2002) apresenta o seguinte texto sobre a definição de *spam*:

> Para começar, *spam* não é *e-mail* comercial não solicitado. Se alguém em meu bairro ouve que eu estava procurando por uma antiga Raleigh de três velocidades em bom estado e me envia um *e-mail* oferecendo uma para me vender, eu ficaria contente, e ainda sim, este *e-mail* seria comercial e não solicitado. A característica definidora de spam (de fato, a razão de ser) não é que ele é não-solicitado, mas que ele é automatizado. É meramente incidental também que o spam é usualmente comercial. (GRAHAM, 2002, tradução nossa)

Para este trabalho, será adotada a seguinte definição de *spam*:

> [...] considera-se *spam* como o recebimento de mensagens não solicitadas, enviadas através de ferramentas automatizadas ou não para uma ou mais pessoas sem que estas tenham solicitado as informações contidas no mesmo. (FABRE, 2005)

3.2 Tipos de spam

Embora o *spam* tenha ganhado fama pela grande quantidade de mensagens eminentemente comerciais, ou propaganda, atualmente há diversas classes de *spam*. Geralmente cada ferramenta *anti-spam* possui sua lista de classificações de *spam*, tornando assim mais eficiente a detecção quando uma mensagem apresentar características de alguma entrada em sua tabela de classificação.

Uma boa referência a ser seguida para a classificação dos *spams* é dada pelo CGI.BR através de um de seus sites, o Antispam.br[1]. De acordo com o CGI.BR, os *spams* são classificados como:

Correntes (*chain letters*): são mensagens que possuem textos finais que têm como característica principal o pedido para que o usuário, ou seja, o destinatário reenvie a mensagem para outras pessoas de seu contato. Na maioria das vezes as correntes solicitam que a mensagem seja enviada para "todos da sua lista de contatos" ou "todas as pessoas que você ama". O corpo do texto geralmente contém histórias antigas, superstições ou histórias que sempre levam a um "final feliz". Ele também geralmente contém insinuação do tipo: "se você quebrar essa corrente você terá azar".

Boatos (*hoaxes*): são mensagens muito parecidas com as correntes, ou seja, geralmente solicitam que a mensagem seja enviada para "todos da sua lista de contatos" ou algo parecido. O ponto principal de diferenciação de correntes e boatos é o conteúdo. Os boatos geralmente contam histórias alarmantes e falsas. Essas histórias, em geral, ou são difamatórias, denegrindo imagens de empresas, ou prometendo prêmios irrecusáveis, ou filantrópicos, contando histórias de crianças doentes em estágio terminal e informando que, se o *e-mail* não for repassado, a família não receberá ajuda em dinheiro de alguma organização internacional.

Propagandas: são os famosos UCE. São *e-mails* publicitários envolvendo produtos e serviços. É o principal tipo de mensagem que gera polêmica, pois trata da batalha de se fazer propaganda via Internet utilizando *e-mail* sem que este seja caracterizado como *spam*. Apesar de estar havendo uma mudança de mentalidade

[1] O Antispam.br é um site mantido pelo CGI.br e tem como objetivo informar aos usuários e administradores de redes sobre o spam, suas implicações e formas de proteção e combate.

por parte das empresas, muitas ainda fazem propagandas massivas utilizando *e-mails* não solicitados, o que acaba comprometendo a própria imagem da empresa.

Ameaças, brincadeiras e difamação: são mensagens que podem conter ameaças, brincadeiras e principalmente difamação de pessoas, em geral ex-namorados (as), esposos (as), etc.

Pornografia: um dos tipos de *spam* mais conhecidos. Este tipo de *spam* já teve seu tempo de glória e a cada dia o número de mensagens pornográficas diminui. De acordo com o relatório mensal de agosto de 2007 da Symantec (Symantec, 2007), do total de mensagens bloqueadas pelos seus sistemas *anti-spam* de junho a agosto de 2007, apenas 5% foram caracterizados como de conteúdo adulto.

Códigos maliciosos: mensagens que têm como objetivo final a propagação de códigos maliciosos (*malwares)* estão nesta categoria. É crescente o número de *e-mails* propagando códigos maliciosos, principalmente *keyloggers* e *spywares*.

Fraudes: são mensagens que vêm crescendo bastante na Internet. Esse tipo de *spam* geralmente se utiliza de técnicas de engenharia social, tentando convencer o destinatário a fornecer seus dados pessoais, principalmente os financeiros. A quantidade e diversidade desses tipos de mensagens vêm crescendo, pois é cada vez mais difícil atacar os servidores das instituições financeiras. Em vez disso é mais simples e fácil atacar o "elo mais fraco da corrente", ou seja, o usuário final. Os *spams* do tipo fraude se subdividem em dois grandes grupos, o de códigos maliciosos e os de *phishing scam*. As mensagens de códigos maliciosos, como já explicados, geralmente instalam keyloggers e spywares para capturar o que o usuário vê e digita e assim enviar essas informações para um computador coletor de informações. As fraudes que utilizam *phishing scam* estão crescendo cada vez mais, segundo estudo feito pela organização F-SECURE (HYPPÖNEN, 2007) o número de fraudes bancárias no primeiro semestre de 2006 cresceu 55% em relação ao mesmo período de 2005. Grande parte deste crescimento se deu a partir da técnica de *phishing scam*, que consiste basicamente de *e-mails* falsos, passando-se por *e-mails* verdadeiros de instituições bancárias, e que contêm links para sites falsos de bancos, para que seus clientes atualizem seus dados cadastrais e senhas. Com essas informações, os fraudadores fazem transferências bancárias das contas dos usuários para suas próprias contas ou de cúmplices. A própria F-SECURE propõe uma solução simples para tentar diminuir este tipo de fraude. A proposta é a criação

de um domínio *.safe* (como *.bank*) que só poderia ser registrado por instituição financeira credenciada.

Spit* e *spim: os termos *spit* e *spim* significam respectivamente *spam via Internet Telephony* e *spam via Instant Messenge*. Apesar de não serem estritamente *e-mails*, são mensagens eletrônicas enviadas sem solicitação para telefones IP, ou programas de voz sobre IP (VoIP), e programas de mensagem instantânea como ICQ e MSN respectivamente.

***Spam* via redes de relacionamentos**: com a crescente utilização de sites de relacionamentos como o Orkut, surge essa nova modalidade de *spam*. Os *spams* são enviados para os *scrapbooks* (livro de visitas) dos usuários ou através dos *e-mails* enviados por um *spammer* através do sistema de *e-mail* do próprio site de relacionamento.

3.3 Mutações do spam

Existe uma constante luta entre os *spammers* e os desenvolvedores de filtros *anti-spam*. Desde as primeiras mensagens eletrônicas consideradas *spam* até alguns anos atrás, a evolução do *spam* era tímida. Os filtros *anti-spam* que utilizavam apenas as chamadas listas negras, *black-lists*, de palavras eram suficientes para barrar as mensagens escritas unicamente em caracteres ASCII por um prazo razoável. A seleção de duas ou três palavras, unidas pelos conectivos lógicos *and* e *or*, fazia um bom papel para uma série de *spams* que surgiam e circulavam por um período de tempo, até o surgimento de outra variação de *spam* que omitia as referidas palavras-chave.

Devido à rápida mutação de textos e assuntos, foram criadas ferramentas que utilizavam como filtros, algoritmos adaptativos que se moldavam rapidamente às variações de palavras-chave. Além de capturar *spams* escritos puramente em ASCII e gramaticalmente corretos, os algoritmos adaptativos conseguiam detectar uma nova variante de *spam*, aqueles que substituíam letras por alguns números ou símbolos, porém, ainda os tornavam entendíveis pelos destinatários. Um exemplo clássico dessa transformação era a mudança da palavra Viagra para “Vi@gr@”.

Os *e-mails* personalizados foram outra variante do *spam*. Esta inseria saudações no início do *e-mail* baseado no endereço de *e-mail* do destinatário. Com essa inserção, cada *e-mail* era diferente para cada usuário, fazendo com que cada

mensagem possuísse um valor de *hash* diferente, evitando que listas de *hash* de *spams* fossem utilizadas. Apesar de ainda ser utilizada em conjunto com outras mutações, elas em si não foram eficazes por muito tempo devido ao aumento de ferramentas *anti-spam* que utilizavam-se de algoritmos adaptativos e engenhos que identificavam e detectavam linhas de texto não modificadas, que eram posteriormente adicionadas às regras de filtragem.

Uma variante dos *spams* personalizados são os que se utilizavam de textos aleatórios e textos invisíveis. Esses tipos de mensagem utilizavam-se de textos que estavam, em sua maior parte, contidos em *e-mails* comerciais legitimos, ou textos aleatórios, inseridos no início ou fim das mensagens, para tentar evadir-se dos filtros de *spam*. Em alguns casos, essas mensagens utilizavam a codificação *HyperText Markup Language* (HTML) para incluir o texto em letras minúsculas ou até mesmo da cor do fundo da tela.

Por volta do ano de 2005 uma irreverente mutação do *spam* apareceu, o chamado ASCII-*spam*. Este tipo de spam utilizou o criativo conceito de construir figuras utilizando apenas caracteres ASCII. Com isto, palavras que seriam tipicamente detectadas por qualquer filtro *anti-spam* eram escritas na forma de figuras ASCII. A figura 3 mostra um exemplo de como o *spam* era construído utilizando esta técnica.

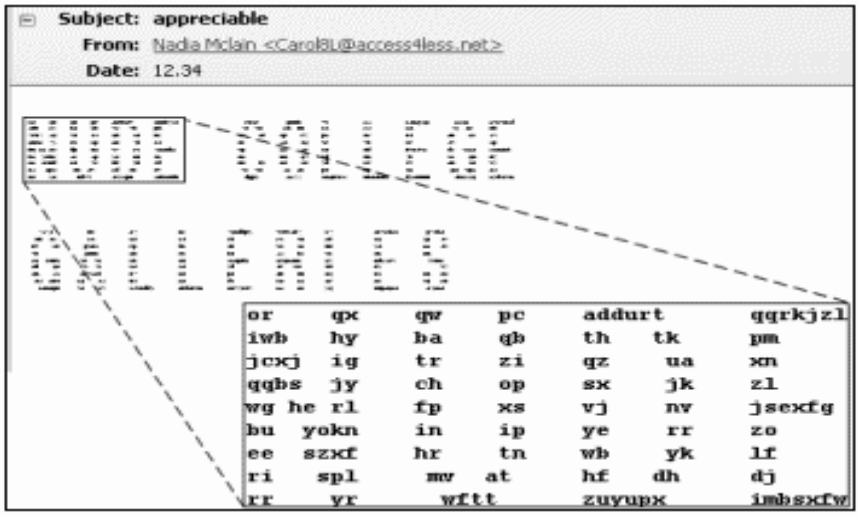

Figura 3. ASCII *spam*. Fonte: Sicurezza Informatica.it[1]

No início do primeiro semestre de 2007 os *spammers* iniciaram uma nova frente de *spam*. As mensagens eletrônicas não mais utilizavam caracteres em ASCII ou HTML, desta vez os *spams* chegavam simplesmente como figuras em anexo. Como a maioria dos clientes de *e-mail* tem capacidade de exibir mensagens anexas

[1] http://www.sicurezzainformatica.it/archives/2005/07/ascii-spam-art.html

no corpo da mensagem, o *spam* era visto pelo usuário final e extremamente difícil de ser detectado pelas ferramentas *anti-spam* que não estavam preparadas para esta nova variação. O problema do *spam* como imagem foi tão grande que, em janeiro de 2007 o volume de *spam* por imagem registrou o incrível índice de 52% do volume total de *spams* (Symantec, 2007).

Após a crescente adequação dos filtros *anti-spam* aos *spams* como imagens, este tipo de mensagem começou a decair. Por volta de junho de 2007, os *spammers* inovaram novamente e começaram a enviar uma nova mutação, os que continham apenas arquivos do tipo Portable Document Format (PDF) como anexos. Mais uma vez as ferramentas *anti-spam* não estavam prontas para mais essa inovação e com isso as caixas postais dos usuários ficaram infestadas com estas mensagens. Informações da Symantec divulgadas pelo IDG Now! informavam que um único *spam* como PDF que tentava estimular a compra de ações foi recebido por mais de 30 milhões de usuários em um período de apenas 10 dias no fim de junho (GARRETSON, 2007). Em 3 de agosto de 2007, o IDG Now! divulgou novas informações, desta vez fornecidas pela empresa Marshal, informando que os *e-mails* com PDF já correspondiam a 25% do total de *spams* em circulação (DUNN, 2007). Como sempre, os filtros *anti-spam* adaptaram-se a esta nova mutação e já é visível o declínio deste tipo de mensagem. Resta agora esperar qual a próxima inovação dos *spammers*.

3.4 Opt-in, double-opt-in, soft-opt-in e opt-out

Se milhões de pessoas acessam a Internet e possuem caixas de mensagens eletrônicas, por que não utilizar esse meio para fazer propaganda? Uma empresa que compra em camelôs, ou sites “especializados”, cds ou até mesmo dvds com imensas listas de *e-mails* pessoais e utiliza programas específicos, os *bots*, para enviar propaganda, ou melhor, *spam*, para esses endereços, está fadada ao ódio dos destinatários das mensagens. Alguns termos foram criados para indicar a política de utilização de mensagens de propaganda por *e-mail* que uma organização adota.

Opt-in é o termo utilizado para a política de envio de mensagens em que é proibido o envio de *e-mails* contendo propaganda, exceto quando isto é previamente aceito pelo destinatário da mensagem. As empresas que adotam o *opt-in* geralmente

possuem em seus sites formulários para cadastro de recebimento de propagandas por *e-mail*.

Double-opt-in ou ***opt-in-confirmado*** é quando além da necessidade prévia de autorização do destinatário dos *e-mails*, a organização envia uma mensagem para o cliente solicitando a confirmação do cadastro. Com esta confirmação, descarta-se o cadastro de caixas de *e-mails* falsas ou do cadastro de *e-mails* de outras pessoas sem autorização.

O ***soft-opt-in*** é semelhante ao *opt-in*, só que adota uma exceção à aceitação prévia para o envio de *e-mails* com propagandas. Esta exceção ocorre quando já existe uma relação, geralmente comercial, entre o remetente e o destinatário.

Opt-out é outro termo utilizado para política de envio de *e-mails* com propaganda. Ele indica que é permitido enviar mensagens com propaganda sem a permissão prévia do destinatário. Também deve ser indicado para o destinatário do *spam* um mecanismo para que ele pare de receber as mensagens. É importante lembrar que *spammers* mal intencionados utilizam o conceito do *opt-out* para criar bancos de dados de *e-mails* válidos para serem vendidos posteriormente. Eles fazem isto enviando *spams* e incluindo links que supostamente retiram o *e-mail* do destinatário da lista do *spam*, mas uma vez que o usuário acesse o link, o *spammer* tem a confirmação de que aquele endereço de *e-mail* ao qual ele enviou o *spam* é válido.

Cada vez mais as empresas sérias e que possuem políticas de bom relacionamento com clientes estão adotando a política de *opt-in* ou *double-opt-in* e incluindo apenas a única característica boa do *opt-out*, ou seja, um mecanismo de exclusão do endereço de *e-mail* do recebimento das mensagens de propaganda.

3.5 Problemas gerados pelo spam

O aumento da largura de banda nos acessos à Internet proporciona um meio mais rápido para os *spammers* despejarem sua imensa quantidade de *spam* por toda a rede. Servidores legítimos de *e-mail* mal configurados também são desejados e, até o presente momento, bastante fáceis de encontrar pelos *spammers*. Os problemas gerados pelo *spam* são bem maiores que a grande irritação dos usuários ao verem suas caixas postais lotadas de mensagens indesejáveis. A seguir é

apresentado um conjunto de problemas causados pelo *spam* elencados pelo CGI.BR:

Não recebimento de *e-mails*: esse problema pode ser causado por diversos fatores decorrentes de *spam*. Em primeiro lugar e decrescendo rapidamente, os provedores de Internet limitavam muito o tamanho das caixas de *e-mail*, com isso, em um único fim de semana era possível ter sua caixa completamente lotada de *spams*, o que impedida o usuário de receber *e-mails* legítimos. Este fator começou a decrescer vertiginosamente após o lançamento do GMAIL pelo Google, que possibilitou encontrar facilmente caixas de mensagens com capacidade maior que 1 Gigabyte de dados. Outro fator é a utilização de filtros *anti-spam*. Com a necessidade de utilização dos mesmos para impedir a entrada de *spam*, os filtros, que não são perfeitos, podem levar a falsos positivos, isto é, *e-mails* legítimos que são classificados como *spam* e por isso impedidos de chegar às caixas de mensagens dos destinatários. Outro fator que pode gerar o não recebimento de mensagens é o de servidores de *e-mail* legítimos mal configurados que são classificados como originadores de *spam*. Com essa classificação, ferramentas *anti-spam* negam o recebimento de mensagens oriundas desses servidores;

Gasto desnecessário de tempo: para cada *spam* recebido pelo usuário, há o tempo necessário para a identificação do mesmo como *spam* e removê-lo de sua caixa de mensagens;

Aumento de custos para o usuário: o usuário final é que termina pagando a conta pelo recebimento de *spam*. Este fator era maior ainda quando não existia o acesso banda larga. Como no Brasil o acesso discado ainda é mais utilizado, o prejuízo é ainda maior, pois para cada *spam* aberto são necessários preciosos segundos de utilização da linha telefônica utilizada para o acesso.

Perda de produtividade: com uma crescente utilização do *e-mail* como ferramenta de trabalho, o *spam* torna-se um dos fatores que diminuem a produtividade no trabalho. O tempo gasto para limpar as caixas de *e-mail*, com o risco de serem apagadas mensagens legítimas, é cada vez maior, principalmente em pequenas empresas que não possuem ferramentas *anti-spam*.

Visualização de conteúdo impróprio ou ofensivo: devido à aleatoriedade do envio dos *spams*, é recorrente a visualização de textos ou imagens caracterizados como ofensivos e impróprios principalmente para as crianças e jovens que a cada dia acessam a Internet mais cedo.

Prejuízos financeiros: esse é visto como o maior problema gerado pelo *spam*. Todos os outros fatores citados podem ou levam ao denominador comum de prejuízo financeiro. Os prejuízos financeiros são gerados pela necessidade cada vez maior do aumento na largura de banda no acesso à Internet, necessidade de servidores com maiores capacidades de processamento de mensagens eletrônicas, aquisição de softwares *anti-spam*, capacitação da equipe de TI para a gerência de soluções *anti-spam*, entre outros. Além disso, o *spam* é o principal meio de divulgação de mensagens fraudulentas que levam ao *phising scam*.

3.6 Estatísticas sobre spam

Devido ao aprimoramento das ferramentas *anti-spam*, alguns poucos e privilegiados usuários não têm a noção da grande quantidade de *spam* que circula na Internet. Os principais agravantes são o rápido aumento da largura de banda das conexões à Internet, a pouca preocupação dos administradores de sistemas de configurarem corretamente os seus servidores de *e-mail* e a falta de cultura dos usuários em relação às boas práticas de utilização do correio eletrônico.

A empresa Symantec produz relatórios mensais sobre vários aspectos de *spam* baseados em dados fornecidos pela sua ferramenta *anti-spam* espalhada em vários servidores pelo mundo. Segundo o relatório de setembro, cerca de 66% de todo o tráfego de *e-mail* na Internet é *spam* (SYMANTEC, 2007). A figura 4 apresenta dados estatísticos da Symantec divididos em categorias, durante meses de junho a agosto de 2007. Essas categorias são utilizadas pela ferramenta *anti-spam* da empresa.

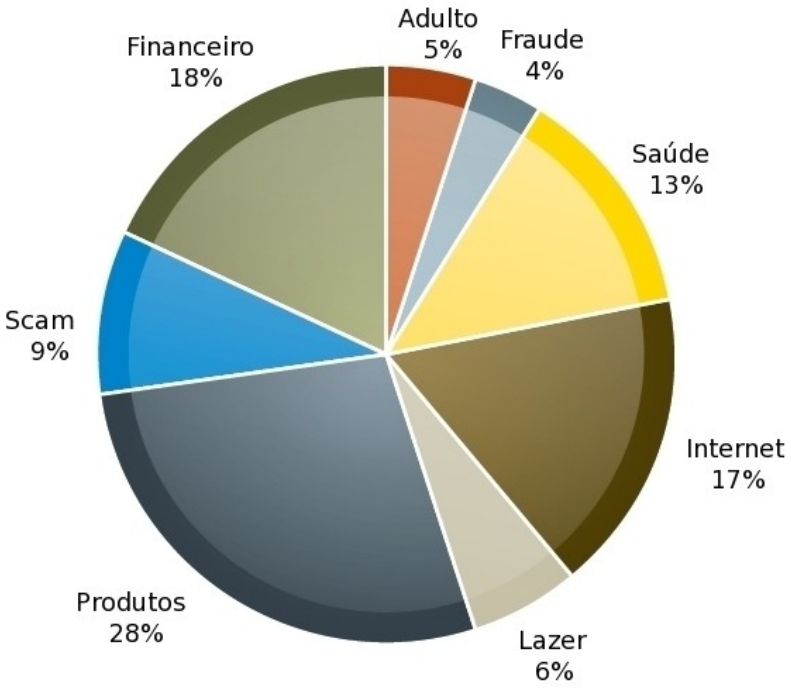

Figura 4. Divisão de *spam* por categoria. Fonte: Symantec[1]

Como apresentado na figura 4, os tipos de *spam* e suas representatividades são:

Produtos (28%): *e-mails* oferecendo produtos e serviços. Exemplo: oferecimento de equipamentos e serviços de investigação;

Financeiros (18%): *e-mails* que contêm referências ou oferecimento relacionados a dinheiro, ações em bolsas de valores ou outras oportunidades financeiras. Exemplos: investimentos e informações sigilosas sobre o estado financeiro de empresas com ações em bolsas de valores;

Internet (17%): *e-mails* que oferecem serviços de Internet ou de computadores. Exemplos: hospedagem de sites e *web design*;

Saúde (13%): *e-mails* anunciando produtos e serviços relacionados à saude. Exemplos: tratamentos médicos para emagrecimento, viagra e aumento de membros do corpo humano;

Scam (9%): *e-mails* fraudulentos que geralmente contam grandes histórias e tentam convencer o usuário de que ele ganhará benefícios se ajudar e fornecer informações privadas. Exemplo: *e-mail* informando que o usuário ganhou na loteria e solicitando dados para efetivar o crédito;

[1] http://www.symantec.com/content/en/us/about/media/leadership/Symantec_State_of_Spam_Report_August_2007.pdf

Lazer (6%): *e-mails* oferecendo jogos, prêmios como viagens e descontos em atividades de lazer. Exemplos: cassinos *on-line*, jogos e viagens.

Adulto (5%): *e-mails* contendo produtos, serviços ou imagens para pessoas acima de 18 anos, geralmente com conteúdo ofensivo ou inapropriado. Exemplos: relacionamentos *on-line* e pornográficos.

Fraude (4%): *e-mails* que parecem ser de empresas de grande conhecimento mas não são. Usualmente são chamados de *phishing scam* e levam os usuários a revelar informações pessoais que geralmente podem levar à perda de dinheiro. Exemplos: *e-mails* passando-se por *e-mails* legítimos de instituições bancárias solicitando recadrastamento de senhas e mensagens de instituições governamentais informando irregularidade em cadastros.

O *Spamhaus Project*[1], uma organização internacional cujo um dos objetivos é rastrear as fontes de *spam*, possui vários servidores espalhados pelo mundo que contêm bancos de dados atualizados em tempo real com listas de endereços IP fontes de *spam*. Esses bancos de dados podem ser consultados *on-line* para fazer bloqueios de *spam* baseados no endereço IP do servidor remetente da mensagem. Dentre os parceiros do projeto estão o *Anti-Phishing Working Group* e o *Federal Bureau of Investigations (FBI)*.

A figura 5 apresenta os dados coletados das últimas 24 horas do dia 3 de setembro de 2007 em relação aos dez países que mais originam spam no mundo. Estes dados são atualizados a cada 24 horas.

[1] Maiores informações sobre o Spamhaus Project podem ser obtidas em http://www.spamhaus.org

Os 10 Países que Mais Originam Spam	
Rank	País
1	Estados Unidos
2	China
3	Rússia
4	Reino Unido
5	Coréia do Sul
6	Alemanha
7	Japão
8	Canadá
9	França
10	Taiwan

Figura 5. Os 10 países que mais originam *spam*. Fonte: Spamhaus[1]

De acordo com a figura os três maiores emissores de *spam* do mundo são Estados Unidos, China e Rússia. Uma importante informação divulgada pelo *Spamhaus Project* é que os países com maiores índices de *spammers* operando dentro de suas redes são geralmente os que possuem pouca ou nenhuma lei sobre *spam*.

O *Spamhaus Project* através do *Register of Known Spam Operations* (ROKSO)[2], que armazena um banco de dados de evidências de grupos profissionais de *spammers*, evidencia que cerca de 80% do *spam* recebido pelos usuários da América do Norte e Europa podem ser rastreados através de endereços, redirecionamentos, localização dos sites e domínios, e levam a um conjunto de cerca de 200 grupos *spammers* já conhecidos. Em setembro de 2007 o ROSKO publicou que os três maiores grupos de *spammers* foram: o *Badcow* composto pelo russo Leo Kuvayev, o grupo ucraniano de Alex Blood, Alexander Mosh, AlekseyB e Alex Polyakov e o grupo de Hong Kong yoric.net composto por Vincent Chan e seus

[1] http://www.spamhaus.org/statistics/countries.lasso
[2] Maiores informações sobre o ROSKO podem ser obtidas em http://spamhaus.org/rosko/index.lasso

parceiros. Segundo os ROSKO, dentre os 200 maiores grupos de *spammers* estão grupos brasileiros, formado pelos *spammers* Flávio Vale, Heik e Agnaldo Rosa de Almeida[1].

Dados estatísticos importantes sobre o *spam* no Brasil podem ser obtidos do site do Centro de Estudos sobre as Tecnologias da Informação e das Comunicações (CETIC.br)[2], um dos grupos de trabalho mantidos pelo CGI.br. O CETIC.br obtém a maioria das informações do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR)[3]. A figura 6 apresenta a quantidade de *spams* reportados ao CERT.br entre 2003 e julho de 2007.

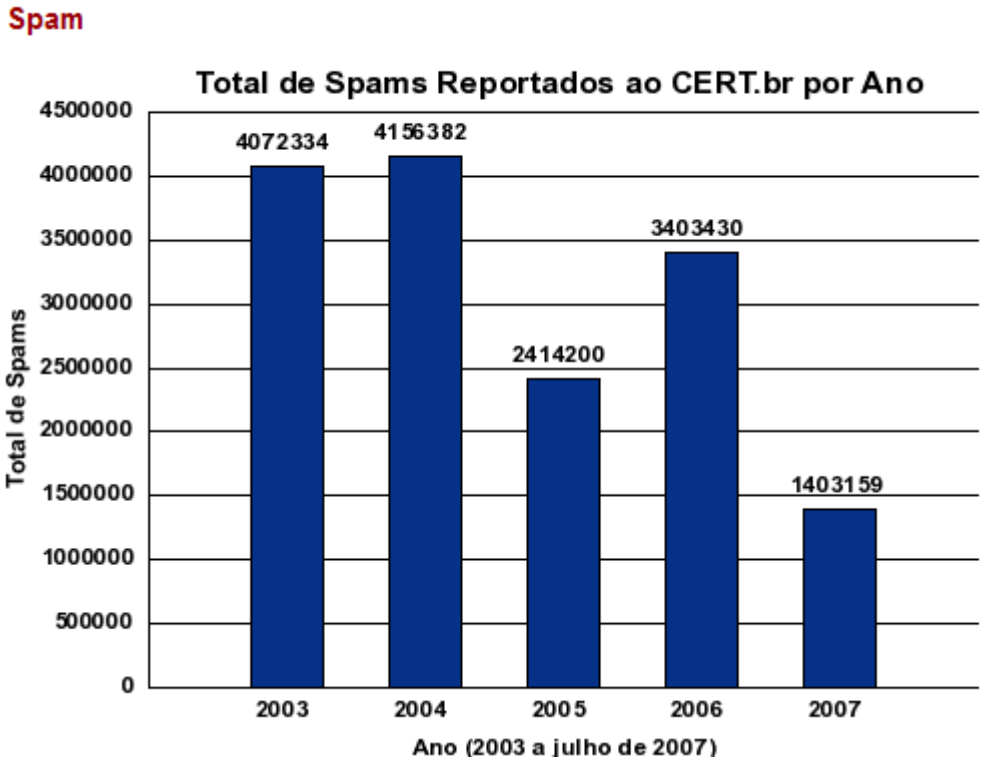

Figura 6. Total de *spam* reportados. Fonte: CETIC.br[4]

Conforme projetado na figura 6, o número de *spam* no Brasil de janeiro a julho de 2007 já ultrapassa um milhão e quatrocentos e três mil mensagens. É importante lembrar que esses números representam a quantidade de *spams* reportados ao

[1] Maiores informações sobre os 200 maiores grupos de spammers podem ser encontradas em http://www.spamhaus.org/rokso/index.lasso

[2] O CETIC.br é responsável pela produção de indicadores e estatísticas sobre a disponibilidade e o uso da Internet no Brasil. Maiores informações em http://www.cetic.br

[3] O CERT.br é responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil. Informações adicionais sobre o CERT.br podem ser obtidas em http://www.cert.br

[4] Disponível em http://www.cetic.br/seguranca/index.htm#spam

CERT.br, ou seja, a quantidade real de *spam* enchendo as caixas postais dos brasileiros deve ser muito maior.

Entre julho e agosto de 2006, o CETIC.br efetuou a 2ª Pesquisa TIC Domicílios e Usuários 2006, realizada anualmente no Brasil. Esta pesquisa foi feita em todas as regiões do Brasil com uma amostra principal de 9.152 respondentes finais, dentre os quais 4.096 eram usuários da Internet. Esta pesquisa avalia vários aspectos sobre tecnologia da informação e comunicações, dentre eles segurança da informação em geral e *spam*. As figuras 7, 8 e 9 apresentam alguns dos resultados desta pesquisa quando o questionamento era sobre *spam*.

A figura 7 apresenta os resultados sobre a freqüência de recebimento de *spam* na principal conta de *e-mail* durante os três últimos meses antes da pesquisa. Cerca de 46,64% dos entrevistados responderam que diariamente recebem *spam*. Este índice foi maior nos entrevistados da região Centro-Oeste, com 54,54% recebendo *spam* diariamente.

Percentual (%)		Diariamente	Toda semana	Todo mês	NS/NR[2]
Total		46,64	38,40	12,85	2,11
REGIÕES DO PAÍS	NORTE/NORDESTE	37,87	43,18	17,10	1,85
	SUDESTE	45,44	39,11	13,32	2,14
	SUL	50,32	36,81	9,16	3,71
	CENTRO-OESTE	54,54	32,60	11,72	1,14
SEXO	Masculino	48,07	38,48	11,37	2,09
	Feminino	44,89	38,31	14,67	2,13
CLASSE SOCIAL[3]	AB	51,13	34,68	11,95	2,25
	C	42,98	41,75	13,88	1,38
	DE	35,38	46,06	13,52	5,03

Figura 7 . Freqüência de recebimento de *spam* na principal conta de *e-mail*. Fonte: CETIC.br[1]

A figura 8 apresenta os resultados sobre o número de *spams* que são recebidos diariamente na principal conta de *e-mail*. O resultado foi obtido pela entrevista dos 455 entrevistados que receberam *spam* diariamente durante os três últimos meses antes da pesquisa. Aproximadamente 70,25% dos entrevistados responderam que recebem de 1 a 10 *spams* por dia.

[1] http://www.cetic.br/usuarios/tic/2006/rel-spam-02.htm

Percentual (%)		1 - 10	11 - 20	21 - 40	41 - 60	+ 60	NS/NR[2]
Total		70,25	13,43	5,94	2,46	5,55	2,38
REGIÕES DO PAÍS	NORTE/NORDESTE	75,95	11,84	5,89	2,63	3,04	0,66
	SUDESTE	66,50	12,42	7,50	2,73	7,11	3,73
	SUL	74,83	13,77	2,70	2,91	5,08	0,71
	CENTRO-OESTE	75,38	10,78	6,33	0,76	4,77	1,99
SEXO	Masculino	65,85	14,76	5,35	3,01	8,41	2,62
	Feminino	76,01	11,68	6,71	1,74	1,79	2,07
CLASSE SOCIAL[3]	AB	70,95	12,68	6,17	3,32	6,10	0,79
	C	67,37	15,09	6,08	1,53	5,14	4,79
	DE	82,18	9,97	2,71		2,71	2,44

Figura 8. Número médio de *spams* diários recebido na principal conta de *e-mail*. Fonte: CETIC.br[1]

Outro dado produzido pela pesquisa e apresentado na figura 9 é sobre o tempo médio gasto diariamente com *spam* na principal conta de *e-mail*. Dos 455 entrevistados neste questionamento, 60,71% gastam entre 1 e 5 minutos por dia com *spam* em sua principal conta de *e-mail*.

Percentual (%)		1 - 5 min	6 - 10 min	11 - 15 min	16 - 20 min	+ 20 min	NS/NR[2]
Total		60,71	23,56	5,73	3,29	3,18	3,54
REGIÕES DO PAÍS	NORTE/NORDESTE	58,60	20,16	10,31	2,24	6,63	2,05
	SUDESTE	57,97	26,17	5,13	3,92	2,49	4,32
	SUL	60,14	27,03	5,06	2,49	2,37	2,91
	CENTRO-OESTE	78,39	12,04	3,05	2,71	2,83	0,99
SEXO	Masculino	63,96	21,80	5,43	1,20	3,32	4,28
	Feminino	56,45	25,86	6,11	6,03	2,99	2,57
CLASSE SOCIAL[3]	AB	60,68	23,04	6,24	3,00	3,67	3,36
	C	61,01	26,51	4,17	3,29	1,94	3,08
	DE	58,97	9,29	10,81	6,08	6,42	8,42

Figura 9. Tempo médio gasto com *spams* por dia. Fonte: CETIC.br[2]

Deve-se considerar que a pesquisa foi realizada no Brasil. Como a maior quantidade de usuários da Internet encontra-se na América do Norte e Europa, esses números podem ser bem maiores nessas regiões.

A empresa SurfControl desenvolveu uma ferramenta *online* que permite simular o custo do *spam* para as organizações. Com esta ferramenta, o usuário pode informar os dados da organização para obter-se tanto o custo do *spam* quanto uma aproximação da quantidade de dias necessários para que o investimento

[1] http://www.cetic.br/usuarios/tic/2006/rel-spam-03.htm
[2] http://www.cetic.br/usuarios/tic/2006/rel-spam-04.htm

despendido na aquisição da ferramenta *anti-spam* da SurfControl seja pago por ela mesma, ou seja, o retorno de investimento. A figura 10 apresenta o cálculo dos custos de uma organização de médio/grande porte que possui 1000 (mil) empregados com caixas de *e-mail*. Considerou-se que a média salarial por hora de cada empregado é de U$3 (três dólares), incluindo impostos, e a média de tempo gasto com *e-mails*, que não estão relacionados à organização, por dia é de 0.1 hora.

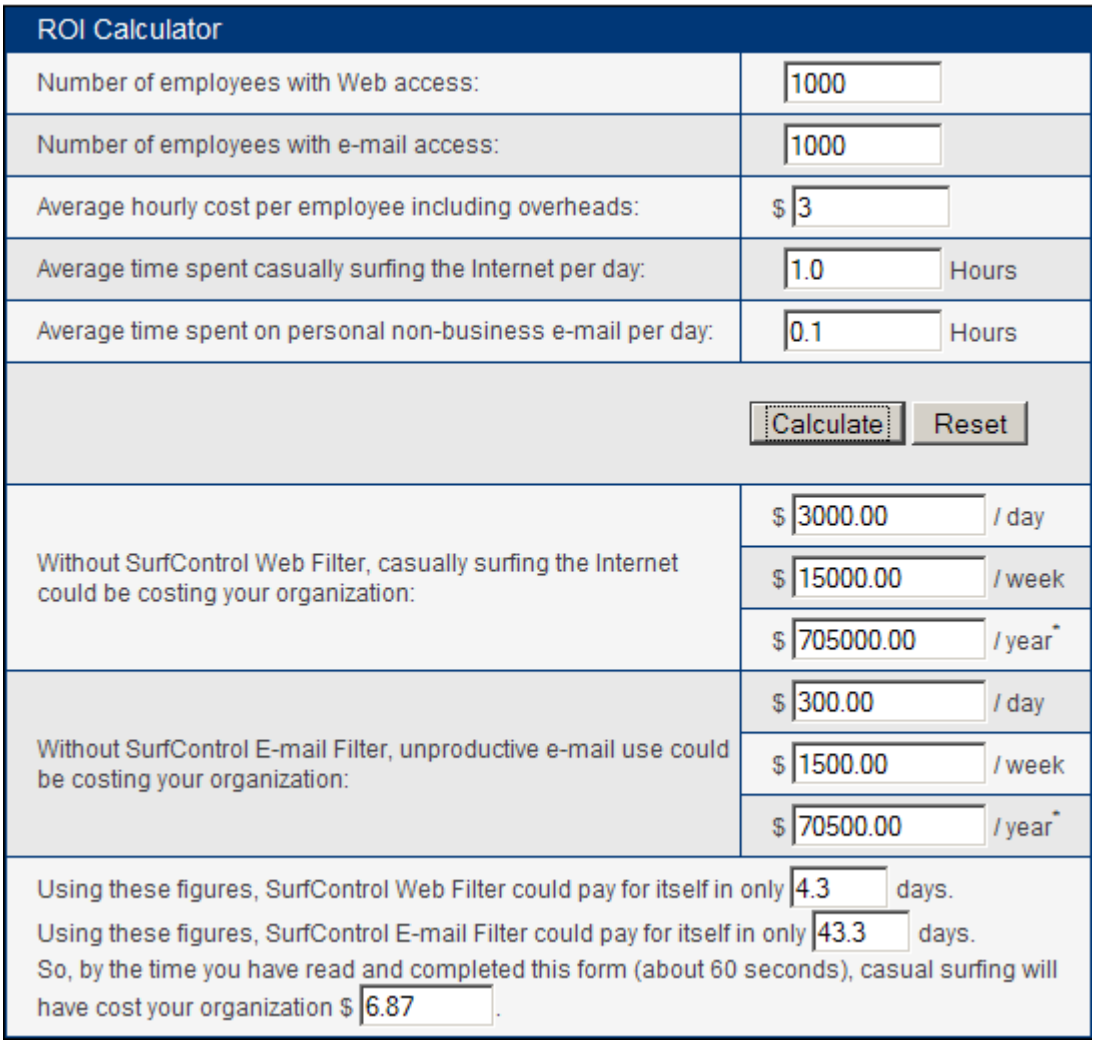

Figura 10. Ferramenta da SufControl para cálculo de custo de *spam*. Fonte: SurfControl[1]

Os resultados apresentados pela ferramenta são impressionantes. Eles mostram o efeito devastador do *spam* para os custos das organizações. De acordo com a simulação aplicada, sem uma solução de *anti-spam* presente, a perda

[1] http://www.surfcontrol.com/general.aspx?id=7136

financeira anual para este cenário, considerando-se um ano com 235 dias, com o *spam* é de aproximadamente U$70.500,00 (setenta mil e quinhentos dólares).

4 TÉCNICAS ANTI-SPAM

A forma mais eficaz de se combater o *spam* é através da criação de leis rígidas para punir penal e civilmente os *spammers*. Como a maioria dos países do mundo não possui e não tem interesse imediato na criação dessas leis, o ônus do bloqueio do *spam* recai sobre os usuários finais, administradores de rede e analistas de segurança da informação.

Como o Estado delegou o problema do *spam* para a sociedade, as ferramentas *anti-spam* são a esperança dos usuários e organizações para diminuir a incidência dessas mensagens indesejáveis, e suas conseqüências, nas caixas *de e-mail*. O principal objetivo dessas ferramentas é verificar todas as mensagens que são endereçadas aos usuários e classificá-las ou não como *spam*.

Pode-se classificar uma ferramenta *anti-spam* de acordo com diversos parâmetros, dentre os quais: facilidade de uso, tanto pelo usuário final quanto pelo administrador de rede; facilidade de suporte ao administrador; oferecimento de listas de bloqueio de endereços IP *on-line*; entre outros. Porém, os dois principais parâmetros que afetam diretamente o usuário final são as quantidades de falso positivo e falso negativo que a ferramenta apresenta diariamente.

Falso negativo significa que uma mensagem foi classificada incorretamente como não sendo *spam*. Se o número de falsos negativos é pequeno, os usuários aceitam a situação sem maiores problemas. Um falso positivo ocorre quando uma mensagem legítima é classificada incorretamente como *spam*. Esta situação é bastante grave, principalmente para pessoas e organizações que efetuam negociações através de *e-mail*.

Atualmente existem várias técnicas *anti-spam* que podem ser utilizadas em softwares livres ou comerciais. É de extrema importância que os responsáveis pela segurança da informação e administradores dos sistemas de correio eletrônico compreendam como as técnicas funcionam, visando escolher a ferramenta que possua técnicas que não impactem no negócio da organização.

4.1 Listas negras on-line

Listas negras são sinônimo de bloqueio imediato. Nelas são armazenadas

informações como endereços IP, domínios e/ou endereços de remetentes que são reconhecidos como fontes de *spam* pelo administrador do sistema de *e-mail*.

Quando uma mensagem chega ao servidor de *e-mail*, a lista é consultada para comparar se alguma de suas entradas é encontrada na mensagem. Caso a comparação seja positiva, a mensagem é imediatamente ignorada com um código de erro definitivo. Caso a comparação da mensagem com a lista negra seja negativa, outras técnicas *anti-spam* podem ser utilizadas caso existam na solução implementada. Uma grande vantagem das listas negras é que as informações cadastradas nelas podem ser obtidas no início de uma transação SMTP, o que garante que um *spam* não consumirá muitos recursos computacionais do servidor receptor.

O grande problema das primeiras listas negras era que cada administrador criava sua própria lista em seu servidor de correio eletrônico. O trabalho de inserir novos endereços IP na lista era muito grande dependendo do volume de tráfego de *e-mail*. Além disso, o administrador tinha que periodicamente rever os bloqueios, pois algum endereço IP que antes era considerado de *spammer* poderia não ser mais.

Por volta de 1997 Paul Vixie[1] criou a *Real-time Blackhole List* (RBL) como um projeto da *Mail Abuse Prevention System* (MAPS)[2]. A RBL era uma lista negra centralizada e alimentada manualmente por uma equipe de administradores. Nela eram armazenados os endereços IP dos servidores utilizados para enviar *spam*. A RBL oferecia serviço de consulta em tempo real gratuitamente através de uma série de comandos formatados para tal objetivo.

A evolução natural para a RBL foi fazer com que as consultas de endereços IP fossem feitas através do protocolo DNS. Com essa nova forma de consulta a lista negra passou a ser chamada de *DNS Real-time Blacklist* (DNSRBL). Atualmente há diversas DNSRBL espalhadas pelo mundo e mantidas por organizações diferentes. Não há um consenso para o termo RBL, alguns chamam de *Real-time Black List* outros de *Real-time Blackhole List* e ainda alguns chamam de *Real-time Block List*. Uma das listas negras de tempo real mais abrangente e consultada no mundo é a *Spamhaus Block List* (SBL) mantida pela *Spamhaus*.

[1] Paul Vixie participou da elaboração de várias RFCs dentre elas a RFC 2052 e RFC 2671 e em 1994 fundou a *Internet Software Consortium* (ISC), hoje *Internet Systems Consortium*, para continuar o trabalho de manter e aprimorar o servidor DNS mais conhecido no mundo, o BIND.

[2] MAPS surgiu como uma organização para prover suporte anti-spam . Em 2005 a MAPS foi adquirida pela empresa Tred Micro e ainda provê serviço de lista negra on-line através de subscrição.

A figura 11 apresenta de forma resumida o funcionamento de uma DNSRBL.

Figura 11. Funcionamento resumido de uma DNSRBL. Fonte: Spamhaus[1]

Quando um servidor de *e-mail* que implementa listas negras de tempo real recebe uma mensagem, ele faz a consulta a DNSRBL através do protocolo DNS para saber se o endereço IP do servidor remetente da mensagem está armazenado como originador de *spam*. O servidor da DNSRBL faz uma busca em sua base de dados e responde se o IP armazenado está ou não no seu banco de dados.

A consulta DNS é feita geralmente invertendo-se o endereço IP do servidor remetente e adicionando a ele o domínio da DNSRBL onde será feita a busca. Por exemplo, se o servidor remetente possui o IP 1.2.3.4 e inicia a entrega de um *e-mail*, o servidor receptor inverte esse endereço transformando-o em 4.3.2.1. Em seguida, o servidor receptor adiciona ao endereço IP invertido o domínio que possui a DNSRBL a ser consultada, por exemplo, 4.3.2.1.dnsrbl.blacklists.com, e faz uma consulta do tipo A[2] ao DNS da lista negra. Se o servidor DNS da lista negra responder com um endereço IP, significa que o endereço IP do servidor remetente da mensagem está presente na lista negra. Se o servidor DNS retornar o código “NXDOMAIN”, significa que o endereço IP do servidor remetente da mensagem não está presente na DNSRBL.

A figura 12 é uma representação mais detalhada da utilização das DNSRBL.

[1] http://www.spamhaus.org/dnsbl_function.html
[2] Uma consulta DNS do tipo A é feita para saber se um determinado host está nos registros DNS do servidor.

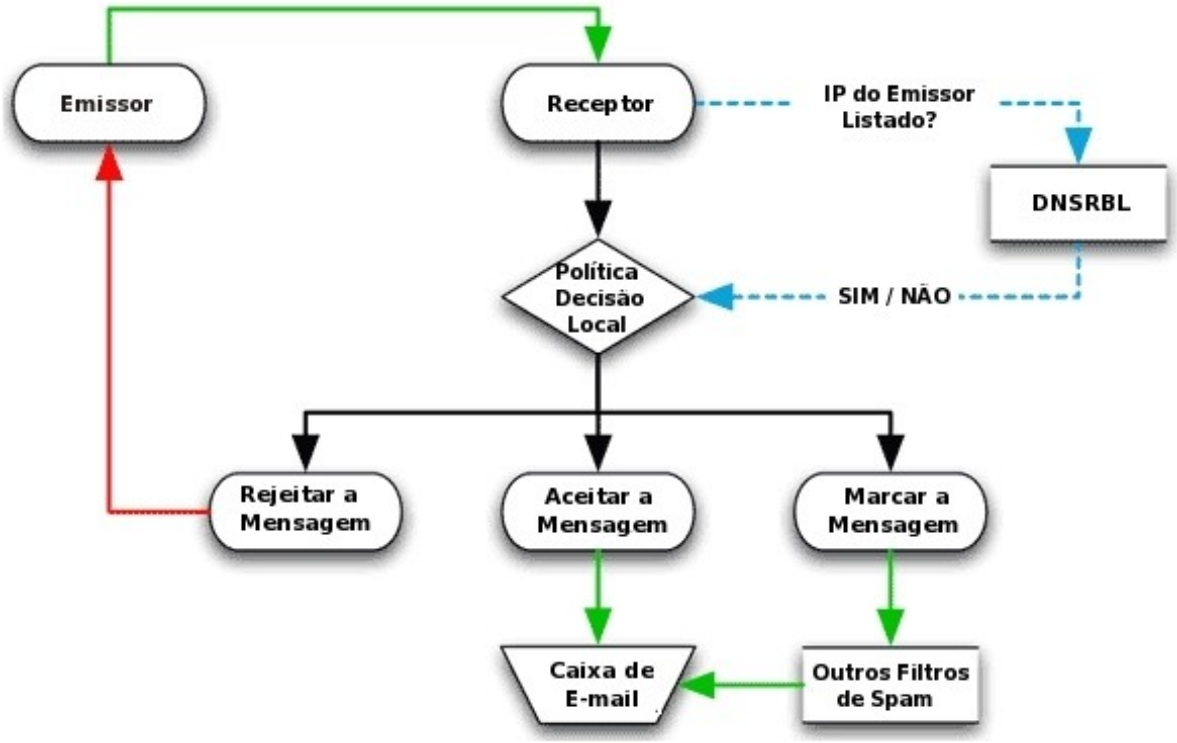

Figura 12. Detalhamento da utilização da DNSRBL. Fonte: Spamhaus[1]

Uma importante consideração que deve ser feita sobre as DNSRBL é que elas apenas informam se um determinado endereço IP está ou não listado nela. De forma alguma a DNSRBL impõe que um endereço IP listado nela deve ser bloqueado. A decisão de bloquear ou não um endereço IP listado em uma DNSRBL é exclusivamente do servidor que está fazendo a consulta. Geralmente os servidores que implementam a DNSRBL oferecem a oportunidade ao administrador de escolher se o bloqueio deve ser efetuado ou não.

4.2 Uso de regras e pesos

Esta técnica consiste geralmente em uma base de regras lógicas que são aplicadas nas mensagens para classificá-las como *spam* ou não. Cada regra define uma ou mais verificações que são aplicadas no *e-mail*. As regras possuem peso, ou pontuação, positivo ou negativo, caso seu retorno seja verdadeiro quando aplicado em uma mensagem.

[1] http://www.spamhaus.org/dnsbl_function.html

Uma pontuação positiva significa que a mensagem testada possui uma maior probabilidade de ser *spam* de acordo com a regra. Caso a regra possua pontuação negativa e sua verificação em uma mensagem resulte em verdadeiro, esta mensagem possui uma menor probabilidade de ser *spam* de acordo com a regra. Um limiar de pontuação é definido para identificar se uma mensagem é *spam* ou não, caso ela o ultrapasse ou não respectivamente. Este limiar, em geral, pode ser ajustado para se adequar ao tipo de *spam* recebido em uma organização.

Geralmente as soluções *anti-spam* que adotam esta técnica já possuem uma base de regras bem formadas que pode atribuir pontuação positiva ou negativa. Quando uma mensagem é checada, todas as regras são aplicadas e a soma da pontuação das regras é feita. Isso significa que mesmo uma mensagem sendo válida para algumas regras de pontos negativos, ela ainda pode ser considerada *spam* caso a soma de todos os pontos resultantes da aplicação da base de regras seja maior que o limiar definido na solução *anti-spam*.

O fator mais importante desta técnica é a base de regras. Para criar esta base é feita uma análise em uma grande amostra tanto de spam quanto de mensagens válidas e selecionadas frases ou palavras características de *spam*. Em seguida deve-se atribuir a pontuação, ou o peso, a cada palavra ou frase levando-se em consideração que elas podem também ser encontradas em mensagens válidas. Se a pontuação for muito alta e a palavra ou frase for encontrada cotidianamente em mensagens válidas o índice de falso positivo poderá ser alto. As ferramentas que utilizam esta técnica geralmente oferecem uma flexibildade grande na construção das regras através da utilização de expressões regulares. As regras também são construídas para verificar a conformidade dos cabeçalhos das mensagens recebidas em relação aos padrões definidos em RFC. Muitos *spams* são bloqueados porque seus cabeçalhos são construídos sem estar em conformidade com os padrões da Internet.

A base de regras que já vem definida nas soluções *anti-spam* em geral reflete o idioma nativo de onde a solução é desenvolvida. Para organizações que recebem *spam* em idioma diferente do adotado pela solução *anti-spam* pode apresentar um elevado índice de falso negativo. Outro fator crítico para a técnica é que geralmente a base de regras original reflete os *spams* que estão em circulação em determinada época. Como o *spam* é altamente mutável, isto é, está em constante modificação de frases, palavras, anexos, entre outros, a base de regras original vai perdendo sua

eficácia ao longo do tempo, exigindo a constante manutenção, ou seja, a criação de novas regras. Se uma organização que adota esta técnica não possui uma equipe experiente e dedicada para construção de novas regras, fatalmente a solução *anti-spam* tenderá a diminuir sua eficácia.

Uma das ferramentas *anti-spam open source* mais utilizadas é o *SpamAssassin*[1]. O *SpamAssassin,* além de outros tipos de verificações, implementa a técnica de regras e pesos. Por padrão o valor do limiar que define se uma mensagem é *spam* ou não é 5. Caso uma mensagem após passar pela análise de pesos e regras obtiver valor igual ou superior a 5 ela é marcada como *spam*, caso contrário ela é marcada como não *spam*. A figura 13 é uma adaptação de (SCHWARTZ, 2004) e apresenta uma mensagem de exemplo que está inserida no código fonte do *SpamAssassin*. Esta mensagem foi escrita para ser considerada *spam* de acordo com uma regra escrita pela equipe de desenvolvimento da ferramenta.

```
Subject: Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
Date: Wed, 23 Jul 2003 23:30:00 +0200
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Precedence: junk
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

This is the GTUBE, the
      Generic
      Test for
      Unsolicited
      Bulk
      Email

If your spam filter supports it, the GTUBE provides a test by which you
can verify that the filter is installed correctly and is detecting incoming
spam. You can send yourself a test mail containing the following string of
characters (in upper case and with no white spaces and line breaks):

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

You should send this test mail from an account outside of your network.
```

Figura 13. Exemplo de uma mensagem considerada *spam* pelo *SpamAssassin*

Ao executar o SpamAssassin em modo de teste para que o mesmo verifique se a mensagem da figura 13 é considerada um *spam* ou não, o resultado é o apresentado na figura 14.

[1] O *SpamAssassin* pode ser obtido gratuitamente através do site http://spamassassin.apache.org

```
Content analysis details:   (1000.0 points, 5.0 required)

 pts rule name              description
---- ---------------------- --------------------------------------------
1000 GTUBE                  BODY: Generic Test for Unsolicited Bulk Email
```

Figura 14. Resultado do *SpamAssassin* para a mensagem da figura 13

Como pode ser observado na figura 14, a mensagem é considerada *spam* pelo *SpamAssassin*, pois o resultado da análise foi verdadeiro para a regra GTUBE, cuja pontuação é de 1000 pontos, ou seja, maior que o limiar padrão de 5 pontos.

Analisando a base de regras do *SpamAssassin*, a regra GTUBE é definida no arquivo de regras 20_body_tests.cf e reproduzida pela figura 15.[1]

```
###########################################################################
# GTUBE test - the generic test for UBE.
body GTUBE        /XJS\*C4JDBQADN1\.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C\.34X/
describe GTUBE          Generic Test for Unsolicited Bulk Email
tflags GTUBE            userconf noautolearn

###########################################################################
```

Figura 15. Regra GTUBE definida na base de regras do *SpamAssassin*

A regra GBUTE definida no *SpamAssassin* foi escrita como uma expressão regular e indica que o teste é feito no corpo do *e-mail* (*body*) e o resultado da regra é verdadeiro se no corpo da mensagem analisada for encontrada a cadeia de caracteres "XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X". O peso da regra GTUBE, 1000, é definido em outro arquivo do *SpamAssassin*, o 50_scores.cf. O Apêndice A apresenta as principais características do *SpamAssassin* e um procedimento de instalação do mesmo para o sistema operacional Linux.

Uma importante adaptação do uso de pesos e regras é que as ferramentas *anti-spam* estão utilizando as outras técnicas existentes como funções embutidas em suas bases de regras. Isto significa que, durante a avaliação das mensagens, as outras técnicas de filtragem, como por exemplo, o resultado de consultas às DNSRBL, em vez de bloquearem imediatamente um suposto *spam*, retornam um

[1] Código fonte do *SpamAssassin* está disponível em http://spamassassin.apache.org/downloads.cgi?update=20070809203

peso para aquele tipo de verificação, o que pode sugerir fortemente que a mensagem, de acordo com a técnica aplicada, é um *spam* ou não.

4.3 Listas Cinzas

Em 21 de agosto de 2003, Evan Harris publicou um artigo que gerou um novo fôlego para o combate ao *spam*. O artigo entitulado "*The Next Step in the Spam Control War: Greylisting*" (HARRIS, 2003) apresentava uma nova técnica chamada listas cinzas. O nome listas cinzas surgiu porque a técnica está entre as listas brancas, em que se cadastram os hosts, endereços de *e-mail* ou domínios que são totalmente confiáveis e passam sem nenhuma verificação *anti-spam*, e as listas negras, nas quais são cadastrados os hosts, endereços de *e-mail* ou domínios que são proibidos de enviarem mensagens para o destino que possui a lista negra.

A técnica foi projetada para satisfazer os seguintes critérios (HARRIS, 2003):

- Possuir o mínimo impacto nos usuários;
- Limitar a habilidade dos *spammers* em burlar o bloqueio;
- Possuir uma manutenção mínima tanto para os usuários finais quanto administradores.

As listas cinzas também tiveram como objetivo de projeto serem implementadas nos agentes de transferência de *e-mails* e não nos usuários finais. Quando publicou o artigo, Evan Harris já havia feito uma implementação da técnica para ser utilizada nos servidores *Sendmail*[1]. Uma importante observação feita por ele é que a técnica não veio para substituir as técnicas atuais e sim complementá-las, tornando o combate ao *spam* mais efetivo.

O que chama a atenção em relação à técnica é sua simplicidade. Para cada tentativa de recebimento de mensagem são retiradas três informações denominadas tripla:

- Endereço IP do host que tenta entregar a mensagem;
- O endereço do remetente no envelope de entrega;
- O endereço do destinatário no envelope de entrega

[1] Maiores informações sobre o Sendmail podem ser obtidas em http://www.sendmail.org

Cada tripla identifica univocamente um “relacionamento” de *e-mail*. A partir dessas informações da tripla a técnica pode ser iniciada.

Analisando as informações que compõem cada tripla e comparando-as com os passos básicos de uma transação SMTP ilustrados na Figura 2, percebe-se que elas podem ser obtidas bem no início de uma transação SMTP, antes mesmo da transferência dos dados que compõem o corpo do *e-mail*. Isto representa um grande benefício, pois garante uma menor quantidade de consumo de recursos do servidor de destino.

Resumidamente a regra básica das listas cinzas é:

> Se nunca tivermos visto esta tripla antes, então recuse a entrega e qualquer outra que possa ocorrer durante certo período de tempo com um código de falha temporária SMTP. (HARRIS, 2003, tradução nossa)

Para que a técnica de listas cinzas seja eficiente e não prejudique o recebimento de *e-mails* válidos, é necessário que os servidores de *e-mail* legítimos sigam as instruções de implementação SMTP de acordo com o padrão definido para o mesmo, ou seja, a RFC 2821. Esta exigência é válida porque esta RFC preconiza que o SMTP é um protocolo de transporte não confiável, por isso prevê a possibilidade de falhas temporárias. Como são possíveis falhas temporárias durante a transmissão de *e-mail*, os servidores que implementam a RFC 2821 devem possuir mecanismos de retransmissão de mensagens.

À época da implementação e testes iniciais das listas cinzas (HARRIS, 2003), foi detectado que a maioria dos *spams* eram enviados por aplicações que adotava a metodologia “atire-e-esqueça”, isto é, elas tentavam enviar o *spam* para um ou mais servidores MX[1] do domínio, mas nunca tentavam fazer retransmissão das mensagens que falhavam, assim como fariam os servidores reais de *e-mail*. Soma-se a esta constatação o fato de que a maioria dos vírus e *worms* que se proliferam por *e-mail* também não realizam retransmissões de mensagens.

Para a implementação das listas cinzas é necessário o armazenamento em um banco de dados com pelo menos os seguintes dados para cada tripla, além dela própria (HARRIS, 2003):

- O tempo que a tripla foi vista pela primeira vez;
- O tempo que o bloqueio à tripla irá expirar;
- o tempo que o registro da tripla irá expirar no banco de dados.

[1] Um servidor MX do domínio é aquele definido por um registro do tipo MX no servidor de nomes para aquele domínio, ou seja, é aquele registrado para receber e-mails da Internet

A figura 16 ajuda a entender o algoritmo das listas cinzas.

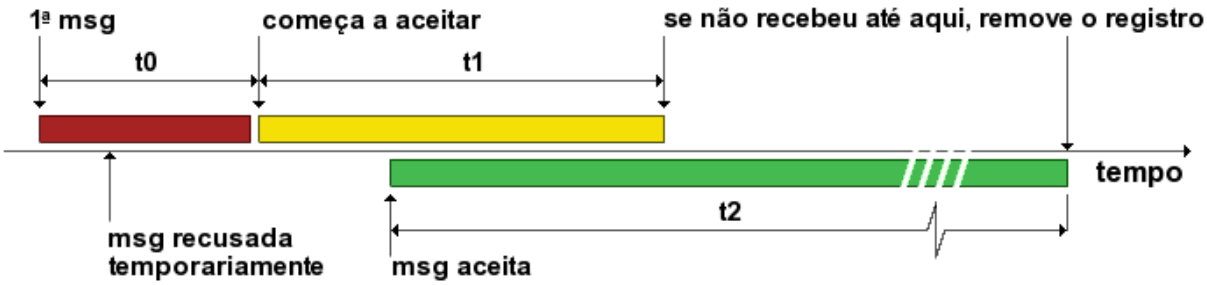

Figura 16. Gráfico de tempo da técnica de listas cinzas. Fonte: Antispam.br[1]

Quando a primeira mensagem de uma tripla é recebida, o servidor remetente recebe um código de erro temporário e a tripla é armazenada no banco de dados do servidor receptor juntamente com os contadores de tempo. Se o servidor remetente reenvia a mensagem antes de expirar o tempo de bloqueio da tripla (t0), ele recebe novamente o código de erro temporário. Expirado t0, o servidor receptor está apto a aceitar a retransmissão da mensagem anteriormente ignorada até que o tempo de registro da tripla expire (t1). Expirado o tempo t1, a tripla é removida do banco de dados. (HARRIS, 2003) ainda estabelece que após aceita a retransmissão de uma mensagem, o endereço IP do servidor remetente e o domínio que ele representa sejam inseridos em uma lista branca juntamente com o tempo de expiração da lista branca (t2). Se durante t2 o servidor remetente não enviar nenhuma outra mensagem o seu registro na lista branca é removido. Caso t2 não expire e uma nova mensagem do servidor remetente seja enviada, ela será aceita imediatamente, sem precisar passar pelo algoritmo da lista cinza, fazendo com que as mensagens não precisem ser retardadas. Além disso, a cada nova mensagem recebida e aceita o tempo t2 é atualizado.

Alguns servidores de *e-mail* implementam uma técnica chamada de *callback* para tentar limitar o problema de endereços de remetentes forjados. Quando implementada, ao receber uma mensagem o servidor receptor tenta validar o remetente iniciando um envio de *e-mail* de volta para o remetente. Se o servidor do remetente indicar que esta conta de *e-mail* não existe, a recepção da mensagem é cancelada. O problema desta técnica é que as listas cinzas, para minimizarem o tráfego dos *e-mails* que serão temporariamente rejeitados, efetuam a ação de

[1] http://www.antispam.br/admin/greylisting/

rejeição depois do comando RCPT, fazendo com que a mensagem de *callback* seja atrasada sem necessidade.

Como explicado em (HARRIS, 2003), felizmente a maioria dos servidores de *e-mail* para implementar o *callback* utilizam o chamando endereço de remetente nulo "<>", para fazer a checagem. Sabendo desta característica, é fácil implementar uma pequena modificação na lógica das listas cinzas, fazendo com que se ocorrer um remetente nulo na transação SMTP, o código de erro temporário deverá ser retornado apenas após o comando DATA ser enviado. Como o teste de *callback* é abortado antes do comando DATA, ele é concluído com sucesso e não é necessário colocar a tripla do *callback* no banco de dados.

As listas cinzas além de ajudar no bloqueio de *spam* têm papel importante na prevenção de ataques do tipo *Directory Harvest Attack* (DHA). O ataque DHA é utilizado pelos *spammers* para tentar encontrar endereços de *e-mail* válidos para o domínio atacado e criar um banco de dados desses endereços que pode ser utilizado posteriormente ou vendido na Internet.

Antes de iniciar o DHA o *spammer* cria uma lista de todas as possibilidades de letras e números até um número de caracteres definido e adiciona o domínio atacado a cada combinação. Em seguida, é iniciada uma transação SMTP com o servidor de *e-mail* do domínio atacado, então, é realizada uma tentativa de enviar *e-mail* para os destinatários da lista anteriormente gerada. Geralmente os servidores de *e-mail* rejeitam os endereços não válidos. Por eliminação, os endereços que não são rejeitados são tidos como válidos e armazenados no banco de dados do *spammer*.

As listas cinzas ajudam na prevenção do DHA porque a maioria dos ataques é executada através de endereços IP dinâmicos. Como grande parte dos *e-mails* iria gerar mensagens de retorno para o *spammer*, uma vez que os destinatários não existiam no domínio, é custoso para o *spammer* efetuar retransmissão neste tipo de ataque. Pelo algoritmo das listas cinzas, uma vez que a tripla do primeiro *e-mail* do ataque não estava no banco de dados, o servidor receptor envia o código de erro temporário para o *spammer* que por sua vez dificilmente irá tentar fazer a retransmissão da mensagem.

4.4 *Sender policy framework* (SPF)

O protocolo SMTP foi escrito de forma que se tornasse fácil o envio e recebimento de mensagens eletrônicas. O mesmo foi escrito sem ter gerado grandes considerações de segurança. A fragilidade do SMTP é hoje vista em diversas formas, porém, uma delas chama a atenção: a facilidade de forjar o domínio remetente de uma mensagem de *e-mail*. Essa facilidade em forjar o domínio remetente da mensagem é muito utilizada pelos *spammers*, que se escondem atrás dessa fragilidade para confundir e eximir-se do ônus do envio de *spam*.

Forjar o remetente de *e-mail* pode levar a conseqüências indesejadas para os usuários da Internet. Quando um *spammer* envia milhares de mensagens com o remetente forjado, mas que é válido na Internet, muitos desses *spams* são destinados a contas de *e-mail* que não existem e, conseqüentemente, o servidor receptor do *spam* envia de volta ao remetente, que é forjado, uma mensagem de erro de entrega de mensagem para cada conta de *e-mail* que não existe. Com isso, o domínio forjado pode receber várias mensagens de erro sem ter tido nenhum envolvimento. Outro problema crítico gerado pela falsificação de remetente é que podem ser imputadas erroneamente a um usuário mensagens de calúnia ou difamação a outro usuário.

Em abril de 2006, foi publicada a especificação final do protocolo *Sender Policy Framework* (SPF), através da RFC 4408. A figura 17 apresenta o algoritmo básico do funcionamento do SPF. Em termos gerais o SPF permite que: o administrador de um domínio defina e publique uma política SPF, onde são designados quais servidores estão autorizados a enviar mensagens em nome do domínio; o administrador de serviço de *e-mail* estebeleça critérios de aceitação de mensagens de acordo com a política SPF publicada para cada domínio consultado. Quando um servidor emissor (Servidor_A) envia uma mensagem para um servidor receptor (Servidor_B) (1), o receptor faz uma consulta DNS para o domínio do usuário contido no campo FROM: da mensagem em busca de uma política SPF para este domínio (2). Se houver alguma política SPF publicada, o servidor DNS do domínio de origem retorna-a para o servidor receptor (3). Este, por sua vez, verifica se o servidor emissor está autorizado, de acordo com a política SPF, a enviar a mensagem que está sendo recebida. Se ele for autorizado, a mensagem é aceita, as outras políticas locais *anti-spam* podem aplicadas e a mensagem é encaminhada para a caixa de mensagens do destinatário (4).

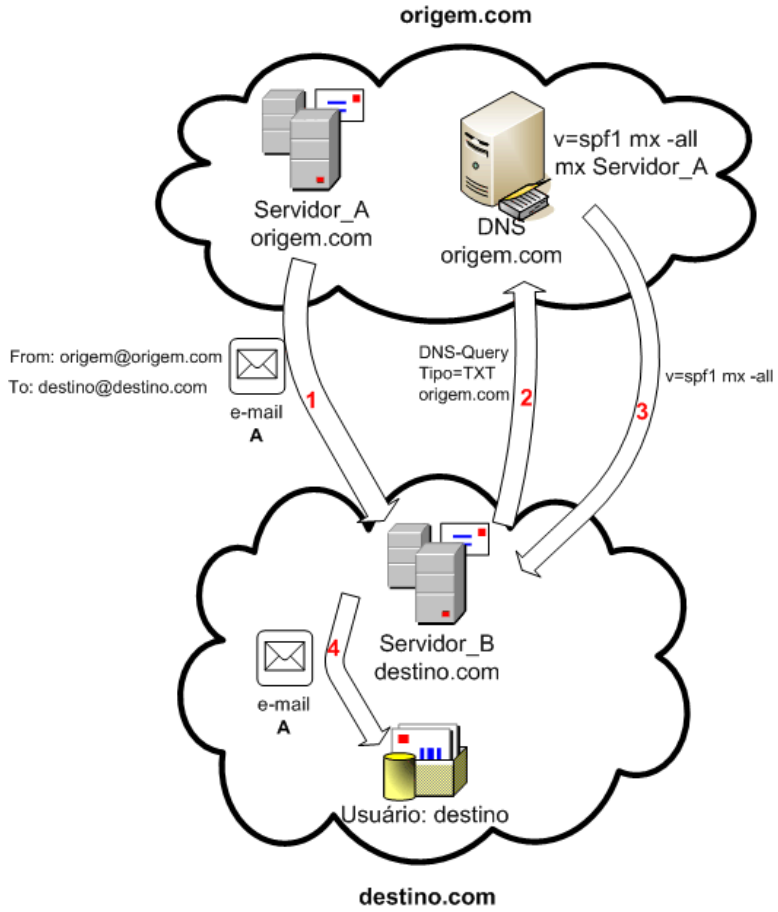

Figura 17. Funcionamento do algoritmo SPF

A RFC 4408 foi largamente baseada no trabalho de Meng Weng Wong e Mark Lentczner. Ela resultou do estudo e fundição de diversos artigos, que tinham a proposta de autenticação de remetente de mensagens eletrônicas, especialmente os de Paul Vixie, "*Repudiating MAIL FROM*", Hadmut Danisch, "*The RMX DNS RR Type for light weight sender authentication*", Gordon Fecyk, "*Designated Mailers Protocol*" e David Green, "*Domain-Authorized SMTP Mail*". Obviamente, após a escrita da proposta da RFC 4408, a mesma foi discutida pela comunidade da Internet através de diversas listas de discussão. (WONG, 2006)

Uma política SPF para um domínio é publicada no servidor DNS deste domínio. Para publicar uma política, o servidor DNS deve possuir um único registro do tipo TXT com uma formatação especificada pela RFC 4408. A IANA[1] criou um novo tipo de registro de recurso DNS denominado SPF, código 99, para a utilização no protocolo DNS. Embora ele também possa ser utilizado e esteja presente na

[1] A IANA é responsável dentre outras atribuições da padronização de domínios DNS. A definição do registro de recurso SPF pode ser encontrada em http://www.iana.org/assignments/dns-parameters

especificação do SPF, a maioria dos servidores de email apenas implementam a checagem do registro do tipo TXT.

Para a escrita de uma política SPF, a RFC 4408 especificou três componentes: mecanismos, qualificadores e modificadores.

A sintaxe básica de uma política SPF definida em um registro DNS do tipo TXT é: "v=spf1 *[([<*qualificador*>]<*mecanismo*>) / <*modificador*>]"[1]. Os componentes <qualificador>, <mecanismo> e <modificador> serão apresentadas posteriormente.

Um domínio pode definir em sua política SPF nenhum, um, ou vários mecanismos e modificadores, sendo desejável que, por recomendação da RFC 4408, o tamanho do resultado da consulta DNS ao registro do tipo TXT seja menor ou igual a 512 octetos. Mecanismos são utilizados para descrever quais servidores são autorizados pelo domínio a enviar email para a Internet. Cada mecanismo é avaliado da esquerda para a direita. Quando um mecanismo é avaliado, três são os possíveis resultados: ele é compatível, não compatível ou gera uma exceção.

Se o mecanismo avaliado é compatível, o processamento dos mecanismos termina e o valor do qualificador daquele mecanismo é retornado como o resultado. Se o mecanismo não é compatível, o processamento do SPF continua no próximo mecanismo. Se ele gera uma exceção, o processamento do mecanismo é parado e um valor de exceção é retornado. Os mecanismos e suas principais utilizações serão explicados posteriormente.

Cada mecanismo pode ser precedido por um qualificador. A especificação SPF define quatro possíveis modificadores: "+" (*Pass*), "-" (*Fail*), "~" (*SoftFail*) e "?" (*Neutral*). Se nenhum qualificador é explicitamente especificado, o qualificador implícito é o "+", isto é, *Pass*. Se durante a avaliação de um mecanismo o cliente SPF encontrar um erro transiente, como uma impossibilidade de realizar consultas DNS durante a avaliação, deve ser retornado o código de erro temporário, isto é *TempError*. Se o registro SPF consultado não puder ser avaliado corretamente, devido a uma má formatação da política SPF ou, se existir mais de um registro SPF para o domínio, deve ser retornado o código de erro permanente *PermError*.

Uma importante observação é que, se nenhum mecanismo de uma política SPF for compatível para a consulta feita e não existir um modificador "*redirect"*, explicado posteriormente, então, o resultado da avaliação da política SPF é definido

[1] A sintaxe da política SPF foi expressa de acordo com a *Argumented Backus-Naur Form* definida pela RFC 2234. Esta pode ser encontrada em http://ietf.org/rfc/rfc2234.txt

como “?”, *Neutral*. Se um domínio não possui uma política SPF registrada em seu servidor DNS, a falta da política deve ser interpretada pelo servidor receptor como *None*. Um resumo do resultado da avaliação de uma política SPF de um domínio pelo servidor receptor de mensagens é apresentado na tabela 1.

Resultado	**Explicação**	**Ação sugerida**
“+” (Pass)	Pelo registro SPF, o servidor está autorizado a enviar o *e-mail*	Aceitar o *e-mail*
“-“ (*Fail*)	Pelo registro SPF, o servidor não está autorizado a enviar o *e-mail*	Rejeitar o *e-mail*
“~” (*SoftFail*)	Pelo registro SPF, o domínio consultado acredita que o servidor não está autorizado a enviar o *e-mail*, mas não quer impor a rejeição da mensagem. De acordo com a RFC 4408 este qualificado está entre *Fail* e *Neutral*	Aceitar o *e-mail*, mas efetuar testes *anti-spam* mais rigorosos na mensagem
“?” (*Neutral*)	Pelo registro SPF, o domínio consultado não pode ou não quer afirmar quando ou não um IP é autorizado a enviar *e-mail*	Aceitar o *e-mail*
TempError	Ocorreu um erro temporário durante a avaliação da política SPF	Aceitar o *e-mail* ou rejeitar com um código SMTP de erro temporário
PermError	Ocorreu um erro permanente durante a avaliação da política SPF ou existe mais de uma política SPF publicada no domínio	A especificação SPF não define ação para erro permanente

Tabela 1. Os qualificadores dos mecanismos SPF

É importante lembrar que as ações sugeridas para os qualificadores, pela especificação SPF, não são uma imposição ao cliente SPF e sim uma recomendação, ou seja, o cliente SPF possui o livre arbítrio para seguir a ação recomendada ou não.

O mecanismo “*all*” é um teste que está sempre em conformidade com uma consulta. Isto significa que não há mecanismo depois de “*all*”. Geralmente ele é

utilizado como o último mecanismo, isto é, o mecanismo mais à direita em uma política para especificar o mecanismo padrão caso os mecanismos precedentes não gerem conformidade na consulta.

O "*include*" é definido como "*include*:<domínio>". Ele especifica que a política SPF do domínio <domínio> deverá ser consultada para verificar se existe alguma conformidade. Se a consulta à política de <domínio> não retornar nem uma conformidade nem um erro, o processamento continua normalmente na política SPF consultada primeiramente. Se a consulta SPF dentro do domínio <domínio> resultar em um qualificador *Pass* significa que a consulta SPF para o domínio original obteve a conformidade com o mecanismo "*include*" e, então, seu qualificador será retornado. Se a consulta SPF dentro do domínio <domínio> resultar em *Fail*, *SoftFail* ou *Neutral*, significa que a consulta SPF para o domínio original obteve uma não conformidade, forçando a continuação da avaliação dos mecanismos da política SPF do domínio original. Se a consulta SPF dentro do domínio <domínio> resultar em *TempError*, *PermError* ou *None* a consulta SPF para o domínio original também deve retornar *TempError*, *PermError* ou *None*, respectivamente.

O mecanismo "*include* permite que um domínio especifique múltiplos domínios administrativos independentes. Por exemplo, o domínio "meudominio.br" pode enviar *e-mail* utilizando os servidores de *e-mail* dos domínios "seudominio.de" e "aqueledominio.com.br". Nesta configuração, uma política SPF aceitável para "meudominio.br" seria: "**v=spf1 include:seudominio.de include:aqueledominio.com.br -all**". Esta política estabelece que se o servidor enviando mensagens com remetente pertencente à "meudominio.br" for um servidor aceitável pela política SPF do domínio "seudominio.de" ou pela política do domínio "aqueledominio.com.br", então a mensagem deve ser aceita. Caso contrário, a mensagem deve ser rejeitada (-all).

O mecanismo "a" em sua forma mais utilizada é definido como "a[:<nome_dominio>]". Ele especifica que uma consulta DNS do tipo A será realizada para <nome_dominio>. Se o IP do servidor que está enviando o *e-mail* coincidir com o endereço IP retornado pela consulta DNS, então há conformidade com o mecanismo. Um exemplo de política SPF com o mecanismo "a" é definida de acordo com o seguinte exemplo: meudominio.br. IN TXT "v=spf1 +a:responsavel.meudominio.br -all". Este exemplo indica que se o servidor que está enviando a mensagem possuir o endereço IP igual ao resultante de uma consulta

DNS do tipo A para o endereço “responsavel.meudominio.br”, então há uma conformidade com a política e a mensagem deve ser aceita.

A definição mais usual do mecanismo “mx” é “mx[:<dominio>]”. Ele especifica que serão feitas consultas DNS do tipo A de todos os servidores MX de <dominio>. Se o endereço IP do servidor transmissor da mensagem coincidir com o IP de algum dos servidores MX de <dominio>, então há a conformidade com o mecanismo SPF.

O “ptr” é um mecanismo definido como: “ptr[:<dominio>]”. Segundo a especificação, quando este mecanismo é encontrado, deve ser feita uma consulta DNS reversa do endereço IP do servidor remetente da mensagem. Em seguida, é feita uma consulta DNS do tipo A para cada nome de servidor retornado pela consulta reversa. Se o endereço IP de alguma consulta do tipo A for igual ao endereço IP do servidor remetente verifica-se se o domínio ao qual foi feita esta consulta do tipo A coincide com <domínio>. Caso esta última verificação seja verdadeira, há uma conformidade com a política SPF.

Os mecanismos “ipv4” e “ipv6” são definidos e funcionam de forma análoga. Eles são definidos como “ipv4: <IP_versão_4>[/prefixo_mascara]” e “ipv6:<IP_versão_6>[/prefixo_mascara]” respectivamente. Se o endereço IP do servidor remetente coincidir com <IP_versão_4>, ou <IP_versão_6> quando for o caso, ou estiver na mesma rede definida pelos parâmetros do mecanismo, então há a conformidade no mecanismo. Um exemplo da implementação deste mecanismo é: “v=spf1 ipv4:11.5.5.0/24 -all”. Segundo este exemplo, apenas os servidores de *e-mail* cujo endereço IP seja integrante da rede 11.5.5.0/24 são autorizados a enviar mensagens pelo domínio especificador desta política.

O último mecanismo definido em (WONG, 2006) é o “*exists*”, que é especificado como: “*exists*:<dominio>”. Se uma consulta DNS do tipo A for feita para <dominio> e houver o retorno de um endereço IP, não importando qual endereço IP foi retornado, há uma conformidade com o mecanismo. Apesar de parecer uma falha da especificação SPF por não importar qual endereço IP foi retornado, o mecanismo “*exists*” foi projetado para a construção de expressões complexas no parâmetro <dominio> com a ajuda de macros[1] definidas pela RFC4408. Uma expressão complexa pode, por exemplo, fazer com que consultas a DNSRBL sejam feitas através do mecanismo.

[1] Uma macro define uma expansão que pode ser feita para um comando nela definido. Por exemplo, a RFC 4408 especifica que a macro %{i} seja expandida para o endereço IP do servidor remetente da mensagem.

Os modificadores provêem informação adicional para a política SPF. Os modificadores definidos na especificação SPF, isto é, "*redirect*" e "*exp*" podem aparecer em qualquer posição da política SPF, porém, a recomendação é que os mesmos apareçam apenas no final. Eles também não podem aparecer mais de uma uma vez na política.

O "*redirect*" é definido como "redirect=<dominio>". Se todos os mecanismos de uma polítca SPF falharem e houver um modificador "redirect", então, será feita uma nova checagem de conformidade SPF desta vez no domínio <domínio>. O resultado desta nova checagem será então considerado o resultado final na avaliação SPF, com exceção de que se nenhum registro SPF for encontrado em <dominio> ou se <dominio> for um valor formado incorretamente, o resultado será a exceção *PermError* em vez de *None*. Se no domínio meudominio.br existe a política "v=spf1 a:192.5.1.1 a:19.2.2.2 redirect:outrodominio.jp" significa que se o servidor remetente de um *e-mail* pertencente ao domínio meudominio.br não possuir o endereço IP 192.5.5.1 ou 19.2.2.2, então, deve ser feita uma nova verificação SPF, desta vez com a política SPF definida no domínio outrodominio.jp.

Se o modificador "exp", definido como "exp=<dominio>", estiver presente em uma política SPF e, durante uma verificação SPF, o qualificador *FAIL* for o resultado retornado, uma mensagem de retorno resultante do modificador também é retornada. Se o modificador não está presente, então, nenhuma explicação é retornada. A mensagem de erro gerada pelo modificador "exp" é formada fazendo-se uma consulta DNS do tipo TXT para o domínio especificado em <domínio>. Se houver algum erro durante a consulta DNS, ou se nenhum registro TXT existir, ou se mais de um registro TXT for retornado, ou se houver algum erro de sintaxe no texto de explicação, então, a política SPF é processada como se nenhum modificador "exp" existisse. Deve-se atentar ao fato de que a RFC 4408 especifica que se na política SPF houver um mecanismo do tipo "*include*" o modificador "*exp*" a ser utilizado é da política SPF original e não da política do domínio especificado no mecanismo "*include*". Analogamente, quando for executado o modificador "*redirect*", o modificador "*exp*" a ser utilizado é o da política especificada no modificador "*redirect*".

A efetividade do SPF depende de dois fatores fundamentais: a publicação das políticas SPF por parte dos administradores de domínio[1] e a realização das consultas SPF por parte dos servidores receptores de *e-mail*.

O SPF é mais um protocolo que ajuda a diminuir a quantidade de *spam* recebida nas caixas de *e-mail* dos usuários. Essa ajuda resume-se em verificar se o servidor que enviou o *e-mail* recebido é autorizado ou não pela política SPF do domínio a enviar a mensagem. O que o SPF não faz é, dada uma mensagem enviada por um servidor autorizado pela política SPF do domínio do remetente da mensagem, informar se esta mensagem é *spam* ou não.

4.5 *Domainkeys identified mail* (DKIM)

Na busca por uma melhor eficiência na detecção do *spam*, algumas técnicas surgiram com o objetivo de prover a assinatura digital das mensagens que circulam na Internet. As empresas Yahoo! e Cisco desenvolveram por volta do ano de 2004 suas respectivas soluções para assinatura digital de *e-mails*: *DomainKeys* e *Identified Internet Mail* (IIM), respectivamente.

As duas técnicas descreviam basicamente a mesma solução e, para prover uma padronização para a mesma, as duas empresas, conjuntamente com outras grandes influências da Internet como a Sendmail, American OnLine, PGP Corporation, IBM, Microsoft, entre outros, criaram um grupo de trabalho e, em maio de 2007 foi publicada, como resultado do grupo de trabalho, a RFC 4871, denominada *DomainKeys Identified Mail (DKIM) Signatures*.

O DKIM:

> [...] define um sistema de autenticação de *e-mail* no nível de domínio utilizando criptografia de chaves públicas e a tecnologia de chaves em servidores para permitir a verificação da origem e conteúdo da mensagem tanto pelos agentes de transferência de *e-mails* quando pelos agentes usuários de *e-mails*. (ALLMAN, 2007, tradução nossa)

Com esta proposta, o DKIM permite aos domínios assumirem a responsabilidade pelas mensagens enviadas, além de prover mecanismos para que os servidores destinatários das mensagens possam verificar tanto o domínio de

[1] Alguns sites possuem ferramentas que ajudam aos administradores de rede a criar políticas SPF e a verificarem se um domínio possui política SPF publicada. Algumas dessas ferramentas podem ser encontradas em OpenSPF (http://old.openspf.org/wizard.html), MxToolBox (http://www.mxtoolbox.com/spf.aspx) e Kitterman Technical Services (http://www.kitterman.com/spf/validate.html)

cada mensagem recebida quanto a integridade das mesmas, isto é, se nenhuma mensagem foi alterada durante a transmissão. A proteção das mensagens eletrônicas, através da assinatura digital do cabeçalho e corpo do email, definidos pela RFC 2822, pode ajudar no controle global do *spam*.

A figura 18 ilustra o funcionamento básico do DKIM. A descrição do funcionamento é apresentada a seguir:

- Os administradores responsáveis pelo domínio emissor geram um par de chaves pública e privada para assinar todas as mensagens de saída do domínio. A chave pública é publicada no servidor DNS do domínio emissor através de um registro de recurso do tipo TXT (passo “A”). A chave privada é disponibilizada apenas para os servidores de *e-mail* responsáveis pelo envio de mensagens que saem de seu domínio. Esses servidores são chamados de assinadores;
- Quando cada mensagem autorizada é enviada, o assinador, de posse da chave privada, gera a assinatura digital da mensagem. A assinatura é colocada como mais um cabeçalho do *e-mail*, o *DKIM-signature*, respeitando a sintaxe definida na RFC 8222, e a mensagem é enviada para o servidor do domínio receptor (passo “B”);
- Os servidores responsáveis por checarem a assinatura digital contida no cabeçalho *DKIM-signature* são chamados de verificadores. Quando uma mensagem chega ao verificador, este extrai a assinatura digital do cabeçalho DKIM, busca no campo FROM: da mensagem qual o domínio emissor, e faz uma consulta DNS a este domínio em busca da chave pública correspondente à privada que assinou a mensagem (passo “C”);
- De posse da chave pública obtida no servidor DNS do domínio emissor, é feita a verificação da assinatura digital para se ter certeza de que a mensagem foi enviada pelo servidor autorizado do domínio emissor e se a integridade da mesma não foi alterada;
- Por fim, o servidor de *e-mail* receptor, aplica suas políticas locais baseado no resultado da checagem da assinatura digital (passo “D”).

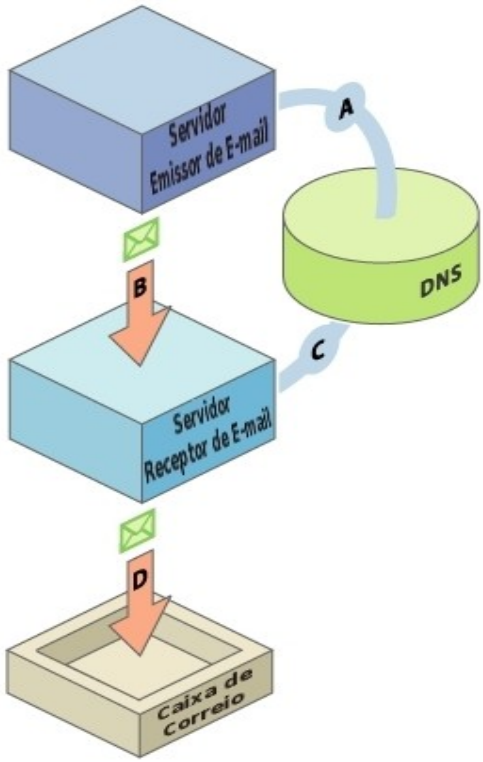

Figura 18. Funcionamento do DKIM. Fonte: Yahoo![1]

Para permitir a utilização de várias chaves públicas para cada domínio, o DKIM suporta um espaço de nomes subdividido através da utilização de seletores. Os seletores podem indicar nomes de localidades (“recife”, “olinda”, “brasilia”), datas de assinaturas de mensagens (“janeiro2007”, “fevereiro2007”), nome de cada usuário do domínio ou quaisquer outros conjuntos de caracteres. Na composição do seletor, pode ser utilizado o caracter ponto (“.”). Isto permite que as chaves públicas sejam publicadas em uma zona de subdomínio do domínio principal das mensagens eletrônicas.

Tanto o registro DNS que contém a chave pública do domínio do emissor da mensagem quanto o cabeçalho *DKIM-signature* das mensagens assinadas têm em sua sintaxe listas compostas de vários campos “identificador=valor”. A composição do campo “identificador” é definida pela RFC 4871 e possui conteúdos diferentes para o registro DNS e o cabeçalho *DKIM-signature*. O campo “valor” é composto de caracteres escritos geralmente em ASCII ou codificados no padrão base64[2]. O

[1] http://antispam.yahoo.com/domainkeys
[2] A codificação de caracteres em base64 é definida na seção 6.8 da RFC 2045, que pode ser obtida em http://www.ietf.org/rfc/rfc2045.txt

caracter ponto-vírgula (“;”) deve aparecer apenas para separar os diversos campos “identificador=valor” nas suas respectivas listas.

Para a assinatura digital das mensagens eletrônicas, a especificação atual do DKIM designa dois possíveis algoritmos: rsa-sha1[1] e rsa-sha256[2]. O algoritmo padrão é o rsa-sha256. A especificação DKIM obriga que os verificadores implementem os dois algoritmos.

Antes de efetuar a assinatura digital, a especificação DKIM impõe que os cabeçalhos e corpo das mensagens passem por um processo de canonicalização. A canonicalização é a formatação do cabeçalho e corpo da mensagem de acordo com o método de ajuste definido. O DKIM especifica dois métodos de canonicalização, o “*simple”* e o “*relaxed*”. O assinador pode utilizar métodos diferentes para canonicalizar o cabeçalho e o corpo do *e-mail*. Os métodos de canonicalização efetuados em uma mensagem são incluídos no cabeçalho *DKIM-signature*, para que o verificador da mensagem possa efetuar os mesmos procedimentos antes de conferir a assinatura digital.

O método “*simple*” efetua pouquíssimas alterações nas mensagens. No cabeçalho das mensagens nenhuma modificação é permitida. Os campos do cabeçalho devem ser apresentados aos algoritmos de assinatura ou verificação exatamente como eles eram na mensagem sendo assinada ou verificada. No corpo do *e-mail*, o método “*simple*” ignora todas as linhas em branco no fim da mensagem. Se não existir corpo do *e-mail* ou nenhum conjunto de caracteres retorno de carro/alimentação de linha (CRLF), um caracter CRLF é adicionado.

O método “*relaxed*” efetua alterações tanto no cabeçalho quanto no corpo das mensagens antes delas passarem nos algoritmos de assinatura e verificação. No cabeçalho, as principais modificações efetuadas pelo método são a conversão de todos os nomes dos campos do cabeçalho para caixa baixa, conversão de todas as seqüências de vários espaços em branco em um único espaço em branco e a remoção de todos os espaços em branco do fim dos valores dos campos do cabeçalho. No corpo das mensagens, a canonicalização “*relaxed*” ignora todos os espaços em branco dos fins das linhas, reduz todas as seqüências de espaços em

[1] As especificações dos algoritmos de *hash* (sha-1) e de criptografia de chaves públicas (rsa) podem ser encontrados respectivamente em http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf e http://www.ietf.org/rfc/rfc3447.txt

[2] As especificações do algoritmo de *hash* (sha-256) podem ser encontradas em http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

brancos em um único espaço em branco e ignora todas as linhas em branco do fim do corpo.

O DKIM permite que seja especificado o tamanho do corpo da mensagem, em número de octetos, que será assinado. Se o tamanho não for especificado, então todo o corpo da mensagem é assinado. Esta funcionalidade permite que servidores com intenso tráfego de mensagens não fique sobrecarregado pela quantidade de assinaturas digitais. Uma preocupação em limitar o tamanho do corpo a ser assinado é que isto permite que um atacante insira qualquer texto que lhe beneficie após o limite do texto que será assinado. O tamanho do corpo da mensagem a ser assinado é calculado apenas depois de ser feita a canonicalização da mensagem.

Como já citado, a assinatura do *e-mail* é armazenada no campo *DKIM-signature* no cabeçalho da mensagem. Ele é composto por uma lista de "identificador=valor" e deve ser escrito e tratado como mais um cabeçalho definido na seção 3.6 da RFC 2822. Este campo deve ser sempre incluído no cálculo da assinatura digital após todos os outros campos do cabeçalho da mensagem a ser assinada. Quando calcular ou verificar a assinatura digital, o valor do identificador "b=" (valor da assinatura digital) da mensagem deve ser tratado como se tivesse um caracter vazio. A tabela 2 apresenta os principais identificadores que podem estar presentes no campo *DKIM-signature* de uma mensagem.

Identificador	Requisito	Descrição
v=	obrigatório	Define a versão da especificação DKIM utilizada na assinatura digital. Deve possuir o valor "1".
a=	obrigatório (pode omitir)	Define o algoritmo utilizado para a assinatura. Os possíveis valores são rsa-sha1 e rsa-sha256. Se omitido, o rsa-sha256 é o padrão.
b=	obrigatório	Contém a assinatura digital da mensagem. O valor do identificador é codificado no padrão base64.
bh=	obrigatório	Contém o resultado da função de hash aplicada ao corpo da mensagem. O valor do identificador é codificado no padrão base64,
c=	obrigatório (pode omitir)	Possui o valor "<metodo1>/<metodo2>" que define respectivamente os métodos utilizados para canonicalizar o cabeçalho e corpo da mensagem. Se omitido o valor "*simple/simple*" é utilizado como

		padrão.
d=	obrigatório	Contém o domínio da entidade que assinou a mensagem. É este domínio que será requisitado a fornecer a chave pública.
h=	obrigatório	Contém uma lista dos nomes, separados por vírgulas, dos campos cabeçalho da mensagem que foram assinados.
i=	opcional	Define a identidade do usuário que originou a mensagem. Também pode conter apenas o domínio ou subdomínio do originador da mensagem.
l=	opcional	Define a quantidade de octetos, depois da canonicalização, do corpo da mensagem que foram incluídos na assinatura digital.
q=	obrigatório (pode omitir)	Define o método de pesquisa da chave pública. Atualmente é o padrão e, se omitido, o único valor definido é “dns/txt”. Este valor indica que a pesquisa deverá ser realizada no servidor DNS do domínio especificado pelo identificador “d”.
s=	obrigatório	Define o seletor a ser utilizado durante a pesquisa DNS para a obtenção da chave pública.
t=	Opcional	Define o tempo em que a assinatura foi criada. O formato é o número de segundos decorridos desde as 00:00:00 de 1 de janeiro de 1970.
x=	Opcional	Define o tempo em que a assinatura digital irá expirar. O formato é o mesmo utilizado no identificador “t”.
z=	Opcional	Contém uma lista, separada por uma barra vertical (“|”), com a cópia dos campos do cabeçalho da mensagem que foram utilizados durante a assinatura da mesma.

Tabela 2. Definição dos identificadores do cabeçalho *DKIM-signature*

A figura 19 mostra um exemplo de um cabeçalho *DKIM-signature*.

```
DKIM-Signature: a=rsa-sha256; d=example.net; s=brisbane;
   c=simple; q=dns/txt; i=@eng.example.net;
   t=1117574938; x=1118006938;
   h=from:to:subject:date;
   z=From:foo@eng.example.net|To:joe@example.com|
     Subject:demo=20run|Date:July=205,=202005=203:44:08=20PM=20-0700;
   bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
   b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
            VoG4ZHRNiYzR
```

Figura 19. Exemplo do campo *DKIM-signature*. Fonte: IETF[1]

A RFC 4871 especificou que a chave pública do domínio para a assinatura das mensagens eletrônicas seja publicada no servidor DNS autorizado do domínio. O registro de recurso DNS é do tipo TXT e tem sintaxe análoga a do campo *DKIM-signature* do cabeçalho das mensagens assinadas. A tabela 3 apresenta os principais identificadores que podem estar presentes em um registro DNS para o DKIM.

Identificador	Requisito	Descrição
v=	obrigatório	Define a versão da especificação DKIM utilizada na assinatura digital. Deve possuir o valor “1”.
h=	obrigatório (pode omitir)	Define os algoritmos de *hash* aceitáveis. Contém uma lista de algoritmos de *hash* separados por vírgulas. Se omitido significa que suporta qualquer algoritmo. Os assinadores e verificadores devem suportar o sha256 e os verificadores também devem suportar o sha1.
k=	obrigatório (pode omitir)	Tipo da chave utilizada. O valor rsa é o padrão se for omitido.
n	opcional	Especifica qualquer texto informativo.
p=	obrigatório	Especifica a chave pública em formato base64.
s=	obrigatório (pode omitir)	Especifica o tipo do serviço ao qual este registro de recurso DNS pode ser aplicado. O único serviço especificado explicitamente na RFC 4871 é “*e-mail*”. Se omitido, este identificador assume o valor “*”, o que significa que pode ser utilizado para qualquer serviço. Este identificador foi elaborado para futuras

[1] www.ietf.org/rfc/rfc4871.txt

		aplicações do DKIM.
t=	opcional	Especifica um ou vários valores separados por vírgulas. Cada valor possui um significado específico. Um importante valor é “y”, que especifica que o domínio em questão está testando a tecnologia DKIM.

Tabela 3. Definição dos identificadores presentes no registro de recurso DNS

Todas as chaves públicas são armazenadas em um subdomínio chamado “*_domainkey*”. Dado um campo *DKIM-signature* com um identificador “d=meudominio.br” e um identificador “s=rsa.pub”, então, o verificador DKIM para obter a chave pública e verificar a integridade da mensagem deverá fazer uma consulta DNS do tipo TXT para “rsa.pub._domainkey.meudominio.br”. As figuras 20 e 21 apresentam respectivamente um cabeçalho *DKIM-signature*, gerado por uma mensagem enviada através do serviço de *e-mail* do Gmail, e uma consulta DNS para obter a chave pública necessária para verificar a assinatura digital apresentada.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
      d=gmail.com; s=beta;
      h=domainkey-signature:received:received:message-id:date:from:to:subject:mime-version:content-type;
      bh=4Ru8VmwyVEVmECOn1rAhDr3536/qxRaLcXEpU6UOnAA=;
b=Y/EFzr8eGY1AJ7sOFq4g4Djrohdag0djGjlToXnRdApPZGUCfeDtS415RaHltD4PI71VuDWOXAU0HDyXbDzVC
bLjMyUelJpDZUhr1Ujp6PzD4KmK6JlRDbPjjEH7JfvOlO4wkbmFCNhzx+icdBqey4jnhJzHClAme8azMkpzhl=
```

Figura 20. Cabeçalho DKIM-signature gerado por uma mensagem enviada através do serviço de email do Gmail

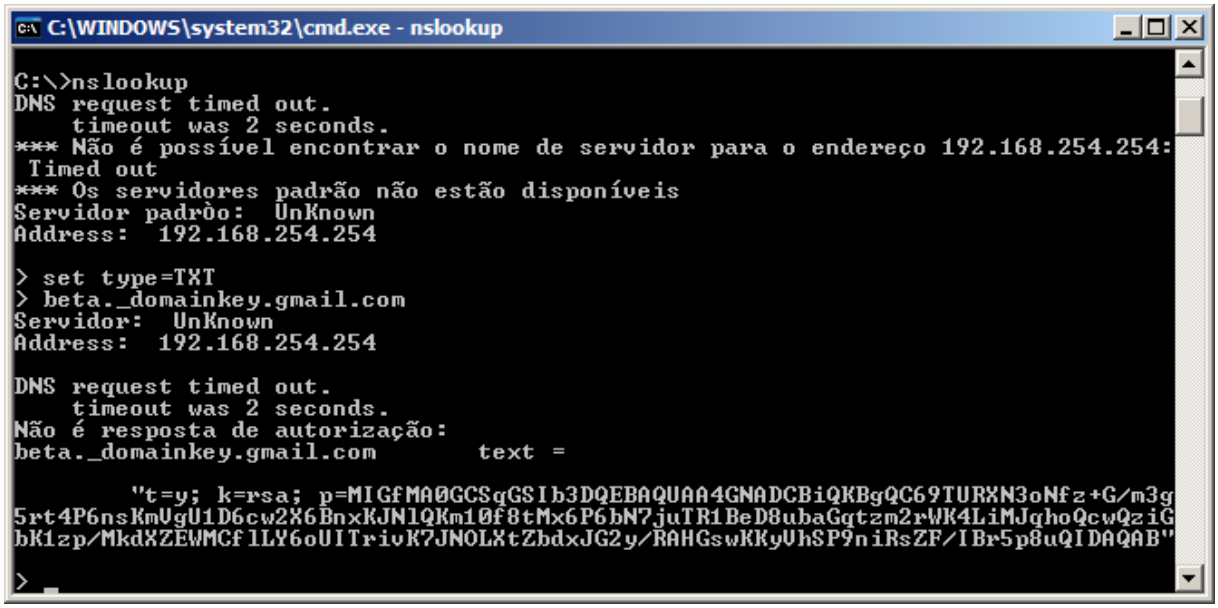

Figura 21. Consulta DNS para obter a chave pública utilizada no DKIM

Para efetuar a assinatura digital das mensagens enviadas, o servidor assinador deverá efetuar os seguintes passos para cada mensagem:

- Selecionar uma chave privada e seu correspondente seletor;
- Determinar quais campos do cabeçalho da mensagem serão assinados;
- Efetuar as canonicalizações no cabeçalho e corpo da mensagem;
- Calcular o resultado da aplicação da função de *hash* no corpo da mensagem e colocá-lo como valor do identificador “bh” do cabeçalho *DKIM-signature*;
- Calcular o resultado da aplicação da função de *hash* tanto no cabeçalho quanto no corpo da mensagem;
- Aplicar a função de criptografia de chaves públicas com a chave privada selecionada anteriormente no resultado da função de *hash* e colocar o resultado como o valor do identificador “b” do cabeçalho *DKIM-signature*;

Uma vez que o assinador pode, a qualquer momento, remover as chaves públicas utilizadas no DKIM de seus servidores DNS, é recomendado que as verificações das assinaturas digitais ocorram tão logo recebidas as mensagens. Para efetuar integridade da mensagem recebida, o verificador DKIM deverá:

- Validar o campo *DKIM-signature*, para verificar se não há inconsistência ou valores inesperados. Qualquer inconsistência fará com que o campo seja completamente ignorado e um retorno de erro permanente SMTP seja retornado;
- Obter a chave pública. Ela deverá ser obtida utilizando o algoritmo definido no identificador “q”, utilizando-se as informações definidas nos identificadores “d” e “s” do cabeçalho *DKIM-signature* da mensagem;
- Efetuar a canonicalização do cabeçalho e corpo da mensagem de acordo com os algoritmos definidos no identificador “c” do *DKIM-signature*;
- Baseado no algoritmo definido pelo identificador “a”, calcular o resultado da função de *hash* aplicada no corpo da mensagem. Se o resultado da função for diferente do conteúdo do identificador “bh”, o verificador deverá ignorar a assinatura digital e retornar um código de erro permanente SMTP;

- Utilizando o resultado da assinatura digital contida no identificador “b” do cabeçalho *DKIM-signature*, executar a função de criptografia definida no identificador “a” com a chave pública obtida anteriormente. Se a assinatura digital não for validada, o verificador deve retornar um código de erro permanente SMTP. Se a assinatura for válida, o verificador deverá efetuar outras verificações que achar necessário ou encaminhar a mensagem para a caixa de *e-mail* do destinatário.

A utilização do DKIM em escala mundial produzirá bons resultados no combate ao *spam*. Muitos usuários podem questionar o fato dos próprios *spammers* utilizarem esta técnica, porém, utilizando o DKIM, os *spammers* estarão se identificando, o que é a última coisa que eles desejam. Fatalmente uma variação das DNSRBL poderá surgir: os bancos de dados mundiais de domínios que utilizam o DKIM e são fontes de *spam*. Esses bancos de dados irão facilitar a detecção imediata do *spam* pelas ferramentas *anti-spam*, assim como já acontece com as DNSRBL.

5 CONSIDERAÇÕES FINAIS

Uma das maiores necessidades do ser humano é a comunicação. Comunicar-se com outras pessoas através de diversas formas, sejam elas orais, escritas ou desenhadas, enriquece o conhecimento de todos envolvidos neste processo. O advento da Internet fez surgir um novo meio para o processo de comunicação, meio este que encurtou as distâncias mundiais e, hoje, permite que os pontos mais extremos do mundo possam se comunicar.

A evolução da Internet é um processo contínuo. Durante o período de seu nascimento até o presente momento algumas tecnologias destacaram-se, dentre elas as mensagens eletrônicas, ou *e-mails*. O *e-mail* é um dos meios de comunicação mais utilizados no mundo para quem utiliza a Internet. Dos familiares e

amigos que tentam diminuir a distância que os separam aos grandes negócios quase que totalmente fechados através dos *e-mails*, esta tecnologia não pára em sua expansão.

O protocolo de transmissão de *e-mail*, o SMTP, foi o principal popularizador da tecnologia, devido a sua extrema facilidade de utilização. Essa grande facilidade também é seu maior inimigo. A falta de mecanismos intrínsecos de segurança no protocolo permitiu que o *e-mail* fosse utilizado para fins negativos, como o *spam*. Apesar de ter começado apenas como meros aborrecimentos para os seus receptores, o *spam* atualmente causa enormes preocupações por ser um dos principais meios eletrônicos para a execução de crimes como a fraude.

Caminhando lado a lado com a evolução da Internet, o *spam* possui uma evolução em seus números estatísticos que impressiona. Atualmente grande parte do tráfego de mensagens eletrônicas na Internet é *spam*. As perdas financeiras das organizações que utilizam a Internet, decorrentes do *spam*, são impressionantes. A soma financeira da perda de produtividade das pessoas devido ao recebimento, detecção e descarte do *spam* é imensa.

Como uma mudança no protocolo SMTP causaria, inicialmente, um impacto negativo na utilização do *e-mail*, pois, geralmente a agregação de segurança implica em perda de funcionalidade, hoje se tenta combater o *spam* com a utilização de ferramentas *anti-spam* que tentam impedir a chegada deste tipo de mensagem nas caixas de mensagens eletrônicas dos usuários finais.

Existem atualmente diversas técnicas *anti-spam*, cada uma com seu próprio algoritmo, porém, todas com um único objetivo final, prevenir a chegada do *spam* ao usuário final. Para a escolha das técnicas a serem utilizadas, faz-se necessária a análise do ambiente onde elas funcionarão. Geralmente as ferramentas *anti-spam* utilizam um conjunto de técnicas para prover uma segurança em camadas, na qual cada técnica oferece um nível de proteção adicional caso a técnica anterior falhe.

Em uma visão a curto prazo, o fim do *spam* parece impossível. Porém, a utilização massiva de técnicas de autenticação de servidores remetentes e das próprias mensagens, através da utilização de protocolos como o SPF e o DKIM, em conjunto com técnicas tradicionais como as DNSRBL poderiam reduzir drasticamente o recebimento de *spam* pelos usuários finais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALLMAN, E. et. al. **DomainKeys Identified Mail (DKIM) Signatures**. IETF, [S.l.], 2007. Disponível em <http://www.ietf.org/rfc/rfc4871.txt> Maio 2007. Acesso em: 01 set. 2007.

BLANZIERI, E.; BRYL, A. **A Survey of Anti-Spam Techniques**. Department of Information and Communication Technology, Itália, 2006. Disponível em <http://eprints.biblio.unitn.it/archive/00001070/01/056.pdf>. Acesso em: 05 maio 2007.

COMER, D. **Internetworking with TCP/IP:** Principles, Protocols and Architecture. 4 ed. New Jersey: Prentice Hall, 2000.

CROCKER, D. et al. **Standard for the Format of ARPA Network Text Messages(1)**. IETF, [S.l.], 1977.Disponível em <http://www.ietf.org/rfc/rfc733.txt>. Acesso em: 30 jun. 2007.

CROCKER, D. **Standard for the Format of ARPA Internet Text Messages**. IETF, [S.I.], 1982. Disponível em <http://www.ietf.org/rfc/rfc822.txt>. Acesso em: 21 maio 2007

CROCKER, D. **Email History**. Living Internet, [S.I.], 2000. Disponível em <http://www.livinginternet.com/e/ei.htm>. Acesso em: 30 jun. 2007.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. **ARPA-DARPA: The History of the Name**. DARPA, Estados Unidos, 2006. Disponível em <http://www.darpa.mil/body/arpa_darpa.html>. Acesso em: 25 de junho de 2007

DUNN, J. **E-mails com PDF já são um quinto do total de spams de imagens, diz empresa**. IDG Now!, Brasil, 2007. Disponível em <http://idgnow.uol.com.br/seguranca/2007/08/03/idgnoticia. 2007-08-03.7622283744/>. Acesso em: 18 ago. 2007.

FABRE, R. **Métodos Avançados para Controle de Spam**. UNICAMP, Campinas, 2005. Disponível em <http://www.las.ic.unicamp.br/paulo/teses/20050215-MP-Recimero.Cesar.Fabre-Metodos.avancados.para.controle.de.Spam.pdf>. Acesso em: 21 abr. 2007.

GARRETSON, C. **Após declínio de mensagens com imagens, cresce registro de spam por PDF**. IDG Now!, Brasil, 2007. Disponível em <http://idgnow.uol.com.br/seguranca/2007/07/12/idgnoticia. 2007-07-12.3311217980/>. Acesso em: 18 ago. 2007.

GRAHAM, P. **A Plan for Spam**. Paul Graham, [S.I.], 2002. Disponível em <http://www.paulgraham.com/spam.html>. Acesso em: 17 ago. 2007.

HYPPÖEN, M. **New proposal would secure financial web sites: F-Secure calls on ICANN to enable safer online banking**. F-Secure, Finlândia, 2007. Disponível em <http://www.f-secure.com/f-secure/pressroom/news/fs_news_20070329_1_eng.html>. Acesso em: 18 ago. 2007.

HARRIS, E. **The Next Step in the Spam Control War: Greylisting**. PureMagic, [S.I.], 2003. Disponível em <http://projects.puremagic.com/greylisting/whitepaper.html>. Acesso em: 06 set. 2007.

IDG NOW!. **IDC: Spam, VoIP e SMS podem enfraquecer uso de e-mail para comunicação**. IDG Now, Brasil, 2007. Disponível em < http://idgnow.uol.com.br/internet/2007/04/09/idgnoticia.2007-04-09.3273618710/>. Acesso em: 21 abr. 2007.

KLENSIN, J. **Simple Mail Transfer Protocol**. IETF, [S.I.], 2001. Disponível em <http://www.ietf.org/rfc/rfc2821.txt>. Acesso em: 21 maio 2007.

LEINER, B. et. al. **A Brief History of the Internet**. ISOC, Washington, 2003. Disponível em <http://www.isoc.org/internet/history/brief.shtml>. Acesso em: 25 de jun. de 2007.

LEVITT, M. et al. **What You Can and Should Do About the Rising Cost of Spam**. SurfControl, California, 2004. Disponível em <http://www.surfcontrol.com/general/assets/whitepapers/rising_cost_of_spam.pdf>. Acesso em: 22 abr. 2007.

PETER, I. **The history of email**. NetHistory.info, Brisbane, 2004. Disponível em <http://www.nethistory.info/History%20of%20the%20Internet/email.html>. Acesso em: 30 jun. 2007.

POSLUNS, J; SJOUWERMAN, Stuart. **Inside the Spam Cartel**. 1 ed. Miami, 2004. Syngress.

POSTEL, J. **Simple Mail Transfer Protocol**. IETF, [S.I.], 1982. Disponível em <http://www.ietf.org/rfc/rfc821.txt>. Acesso em: 21 mai. 2007.

RESNICK, P. **Internet Message Format**. IETF, [S.I.], 2001. Disponível em <http://www.ietf.org/rfc/rfc2822.txt>. Acesso em: 21 mai. 2007.

SAMBUCCI, L. **Ascii-spam-art**. Sicurezza Informatica.it, Itália, 2005. Disponível em <http://www.sicurezzainformatica.it/archives/2005/07/ascii-spam-art.html>. Acesso em: 18 ago. 2007.

SOARES, L. et. al. **Redes de Computadores:** Das LANs, MANs e WANs às Redes ATM. 2 ed. Rio de Janeiro: Campus, 1995.

STALLINGS, W. **Network Security Essencials:** Applications and Standards. 2 ed. New Jersey: Prentice Hall2003.

SYMANTEC. **The State of Spam:** A Monthly Report – August 2007. Symantec, California, 20007. Disponível em <http://www.symantec.com/content/en/us/about/media/leadership/Symantec_State_of_Spam_Report_August_2007.pdf>. Acesso em: 04 set. 2007.

TANENBAUM, A. **Redes de Computadores**. Tradução da 4 ed. São Paulo: Campus, 2003.

TAVEIRA, D. et al. **Técnicas de Defesa Contra Spam**. Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Digitais 2006. UFRJ, Rio de Janeiro, 2006. Disponível em <http://www.gta.ufrj.br/ftp/gta/TechReports/TMRD06.pdf>. Acesso em: 05 set. 2007.

TEIXEIRA, R. **O Pesadelo do Spam**. RNP, Rio de Janeiro, 2001. Disponível em <http://www.rnp.br/newsgen/0101/spam.html>. Acesso em: 21 abr. 2007

TEIXEIRA, R. **Combatendo o Spam:** Aprenda a Evitar e Bloquear E-mail Não Solicitados. 1 ed. São Paulo: Novatec, 2004

WONG, M; SCHLITT, W. **Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1**. IETF, [S.l.], 2007. Disponível em <http://www.ietf.org/rfc/rfc4408.txt>. Acesso em: 30 jun. 2007

APÊNDICE A – Instalação da ferramenta *SpamAssassin*

O *SpamAssassin* tem como pré-requisitos de instalação os seguintes itens:

- Sistema operacional Unix ou compatível com Unix;
- Perl (Versão 5.6.1 ou mais recente);
- Compilador C (ex.: gcc)
- Módulos Perl atualizados: ExtUtils::MakeMaker, File::Spec, Pod::Usage, HTML::Parser, Sys::Syslog, DB_File, Digest::SHA1, Net:: DNS, Net::Ident e IO::Socket::SSL.

As instalações abaixo foram testadas no sistema operacional Fedora Core 5.

Download e Instalação do SpamAssassin

O download e a instalação do SpamAssassin podem ser realizados de três maneiras diferentes, são elas:

- através do CPAN (Comprehensive Perl Archive Network);
- manualmente, através do download e instalação do arquivo fonte gzip;
- manualmente, através do download e instalaçãao do arquivo rpm.

Em todas os tipos, foi instalada a versão 3.2.3 do *SpamAssassin*.

Instalação através do CPAN:

Para realizar o download e a instalação do SpamAssassin de uma forma simples e rápida, pode-se utilizar o CPAN (the Comprehensive Perl Archive Network). Os passos são descritos a seguir:

```
#cpan

cpan shell -- CPAN exploration and modules installation (v1.7602)
ReadLine support available (try 'install Bundle::CPAN')

cpan> o conf prerequisites_policy ask
        prerequisites_policy ask
cpan> install Mail::SpamAssassin
```

Após verificar as dependências e pré-requisitos do sistema, o *SpamAssassin* é instalado automaticamente.

Instalação através do arquivo gzip:

Este tipo de instalação permite que os arquivos fontes do *SpamAssassin* sejam compilados. Para realizar o *download*, é necessário acessar o endereço http://www.spamassassin.org e seguir os próximos passos:

```
# tar zxvf Mail-SpamAssassin-3.2.3.tar.gz
# cd Mail-SpamAssassin-3.2.3
# perl Makefile.PL
What email address or URL should be used in the suspected-spam
report
text for users who want more information on your filter installation?
(In particular, ISPs should change this to a local Postmaster contact)
default text: [the administrator of that system] postmaster@example.com
Checking if your kit is complete...
Looks good
Writing Makefile for Mail::SpamAssassin
# make
# make install
```

Instalação através do arquivo rpm:

O *spamassassin* pode ser instalado como um arquivo RPM. Para tanto, o arquivo RPM deve ser construído através do arquivo *.tar.gz*. O spamassassin-3.2.3.tar.gz, pode ser baixado do endereço http://www.spamassassin.org. O sistema operacional Fedora deverá ter instalado o pacote *fedora-rpmdevtools*. Após feito o *download* do arquivo *.tar.gz*, os seguintes passos são necessários:

```
# rpmbuild -tb Mail-SpamAssassin-3.2.3.tar.gz
# cd /usr/src/redhat/RPMS/i386
# rpm –Uvh Mail-SpamAssassin-3.2.3.rpm
```

Após o processo de instalação, o arquivo de configuração do SpamAssassin encontra-se em */etc/mail/spamassassin/local.cf*.

Testando o *SpamAssassin*

Após instalado e configurado, é necessário testar o SpamAssassin para verificar se ele reconhece corretamente uma mensagem como spam. O código fonte do *SpamAssassin* contém dois arquivos que são utilizados para facilitar o processo de reconhecimento de uma mensagem como spam ou não spam. O arquivo *sample-*

nonspam.txt contém uma mensagem de e-mail que apresenta muito poucas marcas de spam. O segundo arquivo, o *sample-spam.txt*, contém uma mensagem de e-mail que inclui uma string GTUBE (Generic Test for Unsolicited Bulk Email), que é utilizada para validar ferramentas anti-spam.

Para testar o *SpamAssassin*, é necessário executá-lo em modo de teste através da passagem do parâmetro *--test-mode* na linha de comando e, em seguida, fornecer um dos arquivos citados anteriormente como argumento padrão de entrada. Após a execução do teste, o SpamAssassin produzirá uma pontuação. Caso esta pontuação coincida com a pontuação de spam requerida, a mensagem é rotulada como *spam*. O exemplo abaixo exibe um teste do *SpamAssassin* utilizando o arquivo *sample-nonspam.txt*, que produz uma pontuação 0.0.

```
$ cd Mail-SpamAssassin-3.2.3
$ spamassassin --test-mode < sample-nonspam.txt
Return-Path: <tbtf-approval@world.std.com>
Delivered-To: foo@foo.com
Received: from europe.std.com (europe.std.com [199.172.62.20])
by mail.netnoteinc.com (Postfix) with ESMTP id 392E1114061
for <foo@foo.com>; Fri, 20 Apr 2001 21:34:46 +0000 (Eire)
...
Content preview: -----BEGIN PGP SIGNED MESSAGE----- TBTF ping for
2001-04-20: Reviving T a s t y B i t s f r o m t h e T e c h n o l o g
y F r o n t [...]
Content analysis details: (0.0 points, 5.0 required)
pts rule name description
---- ---------------------- --------------------------------------------
0.0 LINES_OF_YELLING BODY: A WHOLE LINE OF YELLING DETECTED
```

O exemplo seguinte exibe um teste usando o arquivo *sample-spam.txt*, que produz uma pontuação de 1000.

```
$ spamassassin --test-mode < sample-spam.txt
Received: from localhost [127.0.0.1] by tala.mede.uic.edu
with SpamAssassin (2.60 1.212-2003-09-23-exp);
Sun, 16 Nov 2003 21:38:03 -0600
...
Content preview: This is the GTUBE, the Generic Test for Unsolicited
Bulk Email. If your spam filter supports it, the GTUBE provides a test
by which you can verify that the filter is installed correctly and is
detecting incoming spam. You can send yourself a test mail containing
the following string of characters (in uppercase and with no white
spaces and line breaks): [...]
Content analysis details: (1000.0 points, 5.0 required)
pts rule name description
---- ---------------------- --------------------------------------------
1000 GTUBE BODY: Generic Test for Unsolicited Bulk Email
```

ANEXO A – Spam enviado pelos advogados Laurence Canter e Martha Siegel

---
From: nike@indirect.com (Laurence Canter)
Newsgroups: comp.graphics.animation,fr.comp.os.linux
Subject: Green Card Lottery- Final One?
Date: 12 Apr 1994 07:52:28 GMT
Organization: Canter & Siegel
Lines: 34
Message-ID: <2odjvs$2ur@herald.indirect.com>
NNTP-Posting-Host: id1.indirect.com

Green Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal program giving away a certain annual allotment of Green Cards to persons born in certain countries. The lottery program was scheduled to continue on a permanent basis. However, recently, Senator Alan J Simpson introduced a bill into the U. S. Congress which could end any future lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE SOON, BUT IT MAY BE THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY FOR FIRST TIME.

The only countries NOT qualifying are: Mexico; India; P.R. China; Taiwan, Philippines, North Korea, Canada, United Kingdom (except Northern Ireland), Jamaica, Domican Republic, El Salvador and Vietnam.

Lottery registration will take place soon. 55,000 Green Cards will be given to those who register correctly. NO JOB IS REQUIRED.

THERE IS A STRICT JUNE DEADLINE. THE TIME TO START IS NOW!!

For FREE information via Email, send request to
cslaw@indirect.com

--
****
Canter & Siegel, Immigration Attorneys
3333 E Camelback Road, Ste 250, Phoenix AZ 85018 USA

cslaw@indirect.com telephone (602)661-3911 Fax (602) 451-7617
