Universidade Federal do Rio de Janeiro – UFRJ
Escola Politécnica - POLI
Departamento de Eletrônica e Computação - DEL

Disciplina: Redes de Computadores – I - Período 2005/1
Aluno: Rafael Jorge Csura Szendrodi
Professor: Otto Carlos Muniz Bandeira Duarte

O SPAM

"Suas origens, sua evolução e as técnicas para evitá-lo!"

Índice

1. Introdução

Atualmente não há dúvida nenhuma que a prática do **SPAM**, termo esse que designa a prática do envio de E-mails não-solicitados na Internet, independente de ser essa prática considerada ilegal ou não (ou no mínimo anti-ética), é um fenômeno que ganhou proporções tais que praticamente ninguém que tenha um E-mail publicado na Internet, nos dias atuais, esta livre dela.

Muito embora tenha começado de forma bastante simples, rústica e amadora no início, em poucos anos a atividade dita "**SPAMMER**" evoluiu para um nível de profissionalismo tal que em nada ficaria devendo as demais atividades ligadas a área Tecnologia da Informação, como por exemplo administração de redes, segurança de redes, programação visual, etc.

De uma mão-de-obra barata, no início, selecionada entre usuários da Internet para a tarefa de enviar manualmente milhares de E-mails não solicitados por dia, até o profissional (ou equipes de profissionais) especializado em inventar formas novas de "otimizar" o envio do SPAM nos dias atuais, poderíamos seguramente dizer que a "carreira" profissional de SPAMMER foi a que mais cresceu em quase 10 anos do nascimento desta que, por muitos, é considerada uma praga, assim como vírus, worms e hackers.

Contudo, o SPAM não nasceu ao acaso. Ele foi obra de um conjunto de fatores, alguns deles remontando ao final dos anos 70 quando o protocolo SMTP começava a ser desenvolvido, e que culminaram no início das atividades SPAMMERS na metade final do ano de 1996.

Estudar esses fatores, entender a lógica e as motivações por trás desta atividade, saber da dificuldade de se definir o que é um SPAM e, por fim, entender por que é mais difícil ainda se chegar a um consenso legal de como se deve tratar os indivíduos que praticam o SPAM é de suma importância para se implementar medidas cabíveis, quer seja como administradores ou usuários de rede, para reduzir os incômodos diários a que nossas caixas de entrada de E-mails são submetidas (ou seja, nos mesmos).

Desta forma, este trabalho destina-se a introduzir-se e aprofundar-se neste fenômeno diário que consome tanto a nossa paciência quanto a largura da banda do canal de comunicação externo das nossas redes.

2. As origens do SPAM

Para aqueles que pensam que o fenômeno do SPAM é coisa da Internet que se originou apenas a quase 10 anos atrás, diremos que estão bastante enganados pois pensam de forma bastante simplista. As raízes do SPAM são bem mais antigas do que muitos pensam e elas se originam na forma como o principal protocolo de troca de mensagens eletrônicas (E-mails), usado nos dias atuais na Internet, começou a ser desenvolvido no final dos anos 70. Para quem não o conhece, ele se chama **SMTP** (**Simple Mail Transport Protocol** ou **Protocolo Simples de Transporte de Mensagens**).

Mas, antes de falarmos do protocolo SMTP, tenhamos em mente o que era a Internet desde os seus primórdios, entre 1971/1972, até por volta de 1985/1986:

1. Uma **rede de caráter militar**, concebida pelos militares americanos dos anos 60 e **administrada pelo DoD** (Department of Defese) dos Estados Unidos da América;
2. Congregava **organizações militares** da OTAN e aliados, **instituições acadêmicas de ensino superior** e **indústrias voltadas a área militar**;
3. Foi **concebida para funcionar** inclusive **em caso de uma guerra termonuclear** com os países do Pacto de Varsóvia (**União Soviética** e Europa Oriental da cortina-de-ferro);
4. Devido ao colocado acima, **precisava ser eficiente, rápida, fácil de ser mantida** e **com protocolos de comunicação que facilitassem as comunicações militares** no caso de uma III Guerra Mundial;
5. **Não tinha os usuários finais dos dias de hoje** (cidadãos comuns, consumidores de uma sociedade capitalista);
6. **Não tinha empresas de todo e qualquer fim**, incluindo ai as empresas especializadas em venda de material pornográfico, diplomas de curso universitário, etc;
7. **Não tinha televendas, vendas por cartão de crédito na Internet e banco virtual** para fazer operações financeiras de casa;
8. **Não tinha interface gráfica** e **nem World Wide Web** (WWW);
9. Entre os cidadãos comuns, **poucos sabiam que a Internet existia**. E provavelmente interessava aos militares que as coisas assim continuassem.

Como podemos ver, a Internet daquela época, excetuando os conceitos técnicos que a tornam operacional nos dias de hoje, em nada lembra a Internet dos nossos dias atuais. É muito importante termos isso em mente porque entenderemos o que se passava na mente dos idealizadores do protocolo SMTP quando do desenvolvimento deste.

2.1. O protocolo SMTP, uma análise sucinta

O SMTP (Simple Mail Transport Protocol) foi proposto inicialmente por Jonathan B. Postel e Suzanne Sluizer na RFC-772 [18] datada de setembro de 1980, sob o título de Mail Transfer Protocol, e posteriormente, após a publicação das RFC-780 [19] e RFC-788 [20], tomou a sua **forma atual** na publicação da **RFC-821** [21] e mais recentemente foi atualiza pela **RFC-2821** [22], de autoria de J. Klensin da AT&T Laboratories.

Além dessas RFC [**ver nota abaixo**] acima, mais três devem ser citadas: a RFC-753 (Internet Message Protocol) [23], a **RFC-822** (Standard for the format of ARPA Internet Text Messages) [24] e a **RFC-2822** (Internet Message Format) [25].

As RFC 772, 780, 788, 821 e 2821 referem-se a evolução do protocolo SMTP e as RFC 753, 822 e 2822 referem-se a evolução da padronização dos cabeçalhos das mensagens transportadas pelos protocolos de transporte de mensagens, como o SMTP.

Vale dizer que o protocolo SMTP não foi o único protocolo de transporte de mensagens eletrônicas concebido para a Internet, mas ele foi aquele que, por sua simplicidade e pelo fato de **ter sido desenvolvido dentro** da comunidade da **ARPANET** (a antiga denominação da Internet), acabou sobrepujando o seu principal "rival", o UUCP [32]. Alguns **MTA** (**Mail Transport Agent**) mais antigos, como o Sendmail [10] e o Exim/Smail [13], oferecem suporte para o protocolo UUCP, mas o uso desse protocolo em paralelo com o protocolo SMTP não é recomendado, pois gera reações adversas nos MTA como, por exemplo, misturar endereçamento UUCP com endereçamento Internet.

O protocolo SMTP, como a própria denominação diz, **foi feito para ser um protocolo simples de transporte de mensagens eletrônicas**. Novamente relembrando a mentalidade da Internet na época em que ele foi concebido, **mentalidade MILITAR**, ele **tinha que ser simples** para que, com poucos recursos e em caso de guerra, **as mensagens pudessem ser transmitidas de forma simples e rápida em situações de emergência**.

Dessa forma, observa-se como é simples mandar um E-mail usando-se um simples programa de telnet em um servidor UNIX (**endereços fictícios**):

> telnet mail.foo.org 25
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
220 mail.foo.org ESMTP Sendmail 8.13.4/8.13.4; Sun, 15 May 2005 14:56:33 -0300
helo internal.foo.org
250 mail.foo.org Hello internal.foo.org [10.0.0.2], pleased to meet you
mail from: rafael@foo.org
250 2.1.0 rafael@foo.org... Sender ok
rcpt to: joao@optimize.somewhere.org
250 2.1.5 joao@optimize.somewhere.org... Recipient ok
data
354 Enter mail, end with "." on a line by itself
From: Rafael Candido Brasil <rafael@foo.org>
To: João Castro Rocha <joao@somewhere.org>
Subject: Teste de Mensagem usando SMTP

Isto é um teste!

.
250 2.0.0 j4FHuXWV004974 Message accepted for delivery
quit
221 2.0.0 mail.foo.org closing connection
Connection closed by foreign host.
>

Observe que os **comandos SMTP** estão **grifados em negrito** e foram necessários apenas 4 comandos básicos para se enviar uma mensagem com sucesso: HELO, MAIL FROM, RCPT TO e DATA e ainda o PONTO FINAL para indicar o fim da mensagem.

Isto representa bem a realidade militar da época e **o porque do protocolo SMTP vingar**, por causa da **simplicidade**. Imagine uma situação de guerra em que se precisa enviar uma mensagem rapidamente. Um soldado somente precisaria memorizar 4 ou 5 comandos básicos para trocar uma mensagem eletronicamente.

Outra característica do SMTP, que reflete a realidade da Internet naquela época, e que **mesmo que você não tivesse um servidor SMTP** onde você está localizado, você poderia remotamente acessar um servidor SMTP qualquer que estivesse funcional, mesmo que não fosse o servidor SMTP do endereço de destino, que **a mensagem seria re-enviada para o endereço de destino sem nenhum problema**.

O protocolo SMTP é tão simples, que nenhuma verificação sobre a validade do endereço de origem passado no comando MAIL FROM é feita, porque poderia se presumir que por algum motivo você estivesse enviando o E-mail de um outra rede que não fosse aquela que você costumeiramente utilizasse.

Os campos From:, To:, e Subject:, são incorporados no cabeçalho da mensagem, eles são especificados nas RFC-753, RFC-822 e RFC-2822, junto com vários **outros campos possíveis que são adicionados** a mensagem toda vez que ela **passa por um servidor SMTP**, isto **facilita o rastreamento** de uma mensagem. Porém **nenhuma verificação** é feita sobre a **validade dos campos From: ou To:** da mensagem. O cabeçalho e o corpo da mensagem são separados por uma linha em branco.

Essa aparente **falta de preocupação** com a **verificação de autenticidade** das mensagens nos assustaria hoje em dia, porém devemos lembrar que **naquela época a Internet era utilizada para fins realmente sérios** e não para os fins que muitos fazem dela hoje em dia. **É ai que está o âmago da questão sobre a "fragilidade" do protocolo SMTP**, ninguém naquela época pensou que um dia a Internet tivesse milhões de usuários (naquela época existiam cerca de 100 servidores espelhados pelos E.U.A. e o resto do mundo e talvez algo em torno de 10.000 usuários), ninguém poderia adivinhar que em 10 anos começariam a surgir interfaces WEB, lojas virtuais, etc. Principalmente, ninguém naquela época poderia adivinhar que propaganda poderia ser enviada através de E-mails. Poderia até ter imaginado nesse tipo de coisa, mas pensariam: " - Não! A Internet é coisa de militar, nunca o cidadão comum vai por o nariz nisto aqui! ".

NOTA: O termo **RFC** significa **Request For Comments**, as RFC são normas publicadas pelo grupo IETF (The Internet Engineering Task Force), uma entidade ligada à Internet Society, e que *a priori* devem ser seguidas para o correto funcionamento da Internet. Para um melhor entendimento das RFC, sugerimos acessar o site da IETF (www.ietf.org).

2.2. O Fake-Mail, o ilustre predecessor do SPAM

Por volta de 1987, a Internet começou a se tornar aberta a usuários de fora da estrutura militar-industrial-acadêmica, por iniciativa do governo americano. Várias funções de administração dela, que eram feitas pelo DoD, passaram a Internet Society e de forma não muito rápida no início, primeiro nos E.U.A. e depois no resto do mundo, ela se popularizou.

Por incrível que pareça, nos primeiros anos de sua popularização não houveram registros de problemas similares ao que conhecemos hoje por SPAM, como se o caráter de seriedade militar da Internet ainda se faze-se valer. Mas vale lembrar que naquela época (1987-1991) a conexão era feita basicamente por modems cuja taxa de transmissão, quando muito, era de 9.600bps, a interface gráfica ainda engatinhava e a World Wide Web estava para ser criada. A banda larga ainda não era economicamente viável para todos.

Por volta do início dos anos 90, **uma brincadeira tornou-se bastante popular** para pregar peças aos novatos. Naquela época **chamava-se Fake-Mail** e era bastante engraçado, já nos dias atuais a conhecemos por denominações menos engraçadas, como fraude, golpe, estelionato e geralmente figura até em páginas policiais dos jornais, visto que usa-se ela para enganar usuários incautos e lhes roubar o dinheiro.

O **Fake-Mail**, como o próprio nome sugere significa ***correio falso*** é essa brincadeira surgiu do fato do **protocolo SMTP ser bem simples** e **não fazer verificação da veracidade dos dados passados** nos comandos SMTP e nos dados dos campos From: e To: dos cabeçalhos das mensagens.

Um **exemplo prático** de um **Fake-Mail** (**os endereços são ficcionais**):

> telnet mail.foo.org 25
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
220 mail.foo.org ESMTP Sendmail 8.13.4/8.13.4; Sun, 15 May 2005 16:05:20 -0300
helo external.faa.org
250 mail.foo.org Hello external.faa.org [192.168.0.7], pleased to meet you
mail from: silvia@foo.org
250 2.1.0 silvia@foo.org... Sender ok
rcpt to: joao@somewhere.org
250 2.1.5 joao@somewhere.org... Recipient ok
data
354 Enter mail, end with "." on a line by itself
From: Silvia Linhares <silvia@foo.org>
To: João Castro Rocha <joao@somewhere.org>
Subject: Eu te amo!

Estou com vontade de te conhecer gatão!
Aparece depois aqui!

Beijos, Silvia

.
250 2.0.0 j5FHuXWV005984 Message accepted for delivery
quit
221 2.0.0 mail.foo.org closing connection
Connection closed by foreign host.
>

O exemplo acima ilustra bem como o protocolo SMTP, por ter sido concebido numa realidade de Internet militar-industrial-academica, dá margem a sérios problemas que põem em dúvida a autenticidade das mensagens eletrônicas por ele transmitidas numa realidade de Internet "caótica" dos dias atuais.

Apesar de ser uma brincadeira, **o Fake-Mail é considerado o embrião da prática do SPAM**, pois existe uma tênue linha que separa um do outro, **a existência ou não do caráter comercial explicito no corpo da mensagem**, fora isso ambos são tecnicamente semelhantes.

Em verdade, **não demorou muito para se evoluir do Fake-Mail para o SPAM**. Os primeiros SPAMMERS provavelmente tinham visto e praticado a brincadeira do Fake-Mail e provavelmente devem ter se perguntado o por que de não se enviar propaganda daquela forma já que o envio direto de mala-direta eletrônica estava ficando desaconselhável por volta da metade de 1996.

De fato, após o início da popularização da banda larga na segunda metade de 1996, principalmente nos E.U.A., começou-se a registrar os primeiros problemas relacionados aquilo que se chamaria mais tarde de atividade SPAMMER.

3. A evolução do SPAM

Tal qual pôde ser observado acima, **o SPAM não surgiu da noite para o dia** mas foi resultado de um conjunto de fatores que remontam ao final dos anos 70. E da mesma forma que ocorre em muitas outras áreas ligadas a Tecnologia de Informação, as técnicas usadas no SPAM evoluíram para o grau de sofisticação que temos hoje em dia. E continuam a evoluir mais e mais ainda.

Algumas perguntas podem estar surgindo ao leitor neste momento. **Por que o SPAM tem essa denominação?** Se o SPAM é simplesmente enviar E-mails, de onde vem esse caráter de ilegalidade que muitos vêem nele? O SPAM é lucrativo?

O **termo SPAM** serve para **designar genericamente** aquilo que tecnicamente é conhecido por **"Envio de E-mails não-solicitados"** (não significa necessariamente uma falha de segurança num sistema ou uma tentativa de invasão do mesmo, como muitos administradores de redes muitas vezes fazem erroneamente tal associação) e **remonta a segunda metade de 1996**, quando as primeiras enxurradas de SPAM começaram a ocorrer. A definição técnica dele poder ser encontrada em diversos sites como o The Antispam Home [1], o MAPS [2], Network Abuse [3], SpamHaus Project [4] e Webopedia [36].

Originalmente **SPAM era uma marca de uma pasta de produto alimentar** a base de carne e bastante famosa [34]. E esse **termo foi pego emprestado** do primeiro filme do **grupo** de rock/comédia inglês **Mount Phyton,** SKETCH (baseado em cenas curtas de comédia) filmado em 1970 [35] [37], **e que mostra uma cena em que** um dos membros do grupo entra nela transvertido como **uma garçonete cantando**, acompanhada por Vikings, **uma música que dizia que todo mundo queria comer SPAM (a comida).** Ao todo **a palavra SPAM foi repetida 94 vezes** nesta curta cena.

Dá para notar a analogia que foi feita com o ato de se enviar E-mails não-solicitados (SPAM) para milhares de endereços com a cena deste filme do grupo Mount Phyton? Como se pode ver, **esse termo pegou assim como**, infelizmente, **o mal-hábito de se enviar milhares de SPAMs todos os dias**.

E sobre o caráter de ilegalidade e sobre se o SPAM é lucrativo? Bem, isso analisaremos mais adiante, no tópico 4 deste trabalho. Por hora vamos nos concentrar na evolução das técnicas de SPAM desde a segunda metade de 1996.

3.1. 1ª Fase: "O SPAM direto e agressivo"

Quando um **maior número de empresas privadas e estabelecimentos comerciais** passou a fazer **uso efetivo da Internet** (grande parte delas poderíamos até chamar de empresas de fundo de quintal ou de garagem), após o "boom" da popularidade da Internet (1991 – 1996), muitas delas **desejaram transpor a mala-direta postal convencional para o sistema de correio eletrônico**.

E o que era o sistema de correio eletrônico em naquele período? Lembrando das origens da Internet, era um sistema sem controle de verificação da validade dos remetentes, que poderia ser utilizado em quaisquer servidores rodando um MTA, etc.

A primeira **atitude destas empresas com relação a mala-direta**, o correio convencional, **e o sistema de mensagens eletrônicas** foi de que **era tudo a mesma coisa**. Desta forma **aconteceu a 1ª fase do SPAM**, mas que **ainda não levava essa denominação**. **O SPAM direto e agressivo** era feito por uma pessoa ou entidade que utilizava sua conta de acesso em um **ISP** (**Internet Service Provider – Provedor de Serviços de Internet**) para mandar mala-direta, **usando o servidor MTA do ISP ou seu próprio servidor MTA**, caso possuísse linha dedicada com a Internet (o que ainda não era muito difundido em 1996).

Claro que como **é muito mais rápido e fácil enviar E-mails** do que cartas postais de mala-direta, muitos usuários da Internet, principalmente os mais antigos, começaram a receber um certo número de **mensagens de propaganda comercial**. Se fosse uma ou duas mensagens por semana, até ai tudo bem. Porém, como o número de empresas na Internet aumentava a cada dia, começaram a **aumentar a freqüência e o numero** de mensagens de propaganda.

Não é de se admirar que em pouco tempo **os usuários**, principalmente os mais antigos e de **instituições militares e de pesquisa acadêmica** (ou seja, de atividades sérias), começassem a **apresentar queixas aos administradores** das suas respectivas redes **para que esse tipo de atividade fosse bloqueada**.

Uma primeira providencia tomada foi **barrar por firewall os MTA dos ISP** que estavam permitindo essa atividade de E-mails comerciais. Estes vendo os problemas causados aos seus demais usuários pelo **bloqueio do serviço de SMTP com outros endereços na Internet**, começaram a fazer novas **clausulas contratuais que proibissem** os seus usuários de enviarem **E-mails com fins comerciais** a partir dos MTA deles **sem o consentimento dos destinatários** que receberiam tais mensagens. Mesmo as empresas que tinham conexões próprias começaram a ter os respectivos servidores SMTP "barrados" por firewall ou por regras configuradas nos MTA dos receptores.

Podemos ver portanto que esta **1ª fase foi de curta duração**, pois alem de ser **facilmente detectável e barrada**, a mala-direta feita dessa forma tinha o inconveniente de deixar o endereço de E-mail e **a identidade do SPAMMER vulnerável e atingível** pelas reclamações dos usuários descontentes em receber SPAM.

NOTA: O termo MTA serve para designar os servidores rodando algum software que protocola transporte de mensagens e não necessariamente um servidor SMTP, ainda que este último na prática domine o transporte de mensagens atualmente na Internet. Para evitar confusão, usarei apenas o termo **servidor SMTP** de agora em diante.

3.2. 2ª Fase: "O SPAM e as máquinas com relay aberto"

Foi na **2ª fase** que o envio de E-mails não solicitados **ganhou a denominação** que tem até hoje, **SPAM**.

Como vimos, o tipo de envio de mensagens da 1ª fase não mais era interessante, principalmente devido ao fato que geralmente o usuário ou entidade, que praticava o SPAM usando os servidores SMTP dos ISP onde tivessem conta, acabavam tendo as contas de acesso encerradas devido a tal prática.

Foi então neste momento que as pessoas ou entidades envolvidas na prática da mala-direta eletrônica **lembraram do famoso trote** de principiante de Internet, **o Fake-Mail**. Relembrando, o Fake-Mail (***correio falso*** ao pé da letra) se vale das "deficiências" ou "fragilidades" do protocolo SMTP, já vistas em 2.1 e 2.2, para enviar uma mensagem eletrônica falsificada utilizando-se de um servidor SMTP próprio ou de terceiros.

Em verdade, até 1996 **ninguém se preocupava** com o fato dos **servidores SMTP terem ou não relay aberto**. Muitos inclusive **achavam benéfico** isso, porque **expressava a natureza de solidariedade global** que a Internet semeava entre os seus membros, ainda que houvessem os Fake-Mails ocasionais..

Infelizmente, isso foi muito mal **utilizado pelos SPAMMERS**, porque valendo-se dessa fragilidade eles poderiam enviar milhares de SPAMs, tais como conhecemos nos dias de hoje, e **quem levaria a culpa seriam os responsáveis pelo servidores SMTP que estivessem com o relay aberto**, pois *a priori*, foram estes que **teriam dado o direito de terceiros enviarem quaisquer mensagens** por aqueles servidores SMTP.

Para dificultar ainda mais o rastreamento da origem de um SPAM por pessoas leigas e se precaver de receber quaisquer reclamações pelas mesmas, os SPAMs passaram a ter algumas características que até hoje, geralmente, observamos neles:

- Normalmente o **campo From: do E-mail é falsificado**, não representando quem realmente enviou a mensagem.
- **Natureza** da mensagem do E-mail é geralmente **comercial**, algumas vezes é golpe contra a pessoa, como as recentes fraudes de E-mails do Banco do Brasil, SERASA e SPC.
- Algums contem apenas números de contato telefônico, algumas vezes com telefones de outros paises.
- Alguns contem um link (atalho) dizendo clique aqui para se descadastrar da lista, que podem ser links válidos e que apenas informam ao SPAMMER que o endereço é válido para mandar mais SPAM ainda.
- Muitos contem um texto, as vezes em inglês, as vezes em português e até as vezes em espanhol, com a mesma mensagem, "Este E-mail está em acordo com o 105º Congresso Internacional de Bases Normativas sobre o SPAM...". Isto nada mais é do que um embuste para dar um "ar de legalidade" ao SPAM enviado.

Como a **maioria esmagadora de servidores SMTP**, entre a segunda metade de 1996 até aproximadamente o início de 1999, **estavam por default com o relay aberto**, ocorreu uma **verdadeira enxurrada de E-mails não solicitados**, que em muitos casos afetou o desempenho de várias redes, principalmente das redes cujos os servidores SMTP

era usados para re-enviar os E-mails não solicitados, a ponto de se comparar com os problemas causados por ataques de vírus ou com pessoas gritando para todos os lados dizendo “Vendo isto! Vendo isto!”. Foi assim que **surgiu a alcunha “SPAM”**, devido a analogia com o filme do **grupo Mount Phyton**.

Atualmente, segunda metade de 2005, a maioria dos servidores SMTP estão configurados com o relay fechado para uso de terceiros, por default, embora ainda seja comum a utilização de máquinas com relay aberto para envio de SPAM. Isso se deve ao fato que muitas máquinas em funcionamento ainda são antigas e não houve preocupação, por parte dos responsáveis pelas mesmas, em fazer-se a atualização delas. Some-se a isto o fato que muitos administradores de redes, por inexperiência, deixam por default máquinas com relay aberto, que são presas fáceis para os SPAMMERS.

Infelizmente tem-se visto isto acontecer até hoje em várias instituições publicas e privadas brasileiras, inclusive na UFRJ – Universidade Federal do Rio de Janeiro.

3.3. 3ª Fase: "O SPAM e as faixas de IPs temporário"

Após terem explorado a exaustão a grande quantidade de máquinas com relay aberto, surge no início de 1999, principalmente com a **franca expansão do serviço de "Internet Banda-Larga"**, mais uma nova modalidade de SPAM que mascarava e dificultava ainda mais a identificação de quem o praticava.

Um outro fator que piorou ainda mais a prática do SPAM nessa fase foi a **expansão do número de empresas do ramo de provimento de acesso à Internet**, muitas delas que poderíamos até classificar como empresas **interessadas apenas em ganhar dinheiro fácil** com o provimento de Internet barata. A Internet no Brasil sofreu bastante esse período (e ainda sofre pela mentalidade surgida nessa época).

Embora tenham diferenças técnicas entre si, a Internet por IP discado e a Internet de Banda-Larga geralmente fazem uso de conexões de IP temporário (devemos lembrar que a quantidade de números IPv4 é limitada e mal distribuída geograficamente, logo um número IPv4 pode ser considerado como algo valioso). Numa conexão de IP temporário, um IP é dado à uma máquina de um cliente, quando da conexão dele no provedor, de forma aleatória. Isto significa que se o cliente conecta e recebe um IP (por exemplo, 10.12.23.8), se ele desconectar e conectar em seguida novamente não necessariamente receberá este mesmo número IP que recebera antes (por exemplo, pode receber 10.11.3.12).

Veja que devido a isto torna-se **impossível identificar o responsável pelo envio de um SPAM** ou pela utilização indevida de máquinas com relay aberto, **sem o auxilio tácito dos responsáveis pelo provedor** que oferece o serviço de acesso. Infelizmente, tem-se observado bastante que, entre ajudar a resolver o problema causado pelo SPAMMER ou continuar recebendo o dinheiro mensal das conexões (que muitas vezes são taxadas pela utilização de banda feita pelo cliente), muitos ISP preferem a segunda opção.

E para ilustrar ainda mais como esses ISP "mercantilizaram" a Internet, podemos citar que muitos deles nem mesmo se preocupam em configurar minimamente os seus servidores dentro os padrões exigidos pelas normas. Por exemplo, o **DNS reverso**, previsto na RFC-1912, é **solenemente ignorado** por muitos provedores de acesso e/ou de serviços, mesmo por muitos provedores famosos como o HotMail. Porém o DNS reverso é uma forma rápida de se identificar os responsáveis por uma faixa de números IP, quando se deseja resolver quaisquer problemas que tenham como origem a utilização de um IP daquela faixa (provavelmente é isso que os ISP não querem, serem identificados).

Se nessa 3ª fase os fatores estavam favorecendo bastante os SPAMMERs, um outro veio a somar ainda mais força para eles agora: A prática do **WEB-SPAM** surgiu durante esse período e ela será falada mais adiante.

Atualmente, não há **nenhuma perspectiva que a mentalidade puramente comercial** dos provedores de acesso e/ou serviços **vá mudar a curto prazo**, muito pelo contrário, vemos que o compromisso dos ISP mais antigos com as posturas de combate ao SPAM foram bastante relaxadas, principalmente para fazerem frente a concorrência com os novos ISP. Um bom exemplo disso é que apesar de nos contratos de provimento de acesso constarem de clausulas que proíbam o SPAM, muitos ISP só agem (quando o fazem) após o recebimento de inúmeras e repetidas reclamações, a respeito de SPAMs enviados por seus usuários, feitas por administradores e usuários de outras redes.

Enquanto esse tipo de atitude perdurar, continuaremos a ter problemas com máquinas usando IPs temporários e mandando grande quantidade de SPAMs pela Internet.

3.4. 4ª Fase: "O SPAMMER profissional dos dias atuais"

Nos dias de hoje, os termos **SPAM** e **SPAMMER** se tornou **um verdadeiro palavrão na Internet**. As empresas de renome, apesar de algumas estarem diretamente ligadas à prática do SPAM, procuram não ter sua marca associadas à essa prática.

Mas entre as **empresas de pequeno e médio porte**, sobretudo aquelas que usam a Internet para a venda de produtos, a **utilização do E-mail para a venda de seus produtos** é, muitas vezes, de **vital importância**.

Por isso muitas empresas fazem uso de **terceiras pessoas ou empresas** para fazerem o chamado "jogo sujo" do SPAM, ou seja, elas as contratam (pagando bem) para cuidarem daquilo que, tecnicamente, chamam de **"E-mail Marketing"**.

Assim como em outras áreas ligadas a Tecnologia da Informação, o surgimento da **"profissão" de SPAMMER** como um profissional de experiência na área do **"E-mail Marketing"** era apenas uma questão de tempo. Segundo o SpamHaus, cerca de 120 indivíduos, em todo mundo, são responsáveis por grande parte do trafego de SPAM que circula diariamente na Internet. Em **números "oficiosos"** da SpamHaus, cerca de **75% de todo o trafego de E-mail mundial é SPAM**, o que dá uma idéia bem clara do dinheiro que é movimentado diariamente pela atividade SPAMMER.

Para se ter uma idéia de como é **lucrativo** o negócio do **"E-mail Marketing"**, podemos citar o fato do americano **Jeremy Jaynes**, condenado recentemente a 9 anos de prisão na Carolina do Norte, E.U.A. [33]. Estimasse que esse SPAMMER **enviava diariamente cerca de 10 milhões de SPAMs** fazendo uso para isso de **16 linhas de alta velocidade** para acesso à Internet. Atenta-se para o fato que para se pagar 16 linhas de alta velocidade, **cujo custo anual é bem alto**, deve-se ter um **retorno excelente dos SPAMs enviados**. Em verdade, se apenas 10% desses 10 milhões de SPAMs enviados tiverem retorno, o lucro poderá ser satisfatório.

Na prática é bem **difícil se processar legalmente um profissional do SPAM**. **Não existe ainda uma legislação clara, nem a nível de Brasil e nem a nível mundial**, para crimes relacionados a utilização da Internet. O americano citado acima só foi condenado porque **ele violou uma lei Anti-Spam da Carolina do Norte** que proibi o envio de mensagens utilizando-se em endereços e pseudônimos falsos. Nota-se que foi uma lei aplicada apenas a um estado americano, que **não alcançaria um SPAMMER** que tivesse suas atividades baseadas **em outro país**.

Deve-se ter em mente que, enquanto a nossa meta como administradores e/ou usuários é evitar de recebermos E-mails SPAMs, **a meta dos SPAMMERS profissionais** é tentar **fazer o SPAM chegar** de qualquer forma **no nosso endereço de E-mail**. Muitas das técnicas SPAM mais modernas que existem atualmente foram inventadas por esses "profissionais" de rede, que procuram se aprimorar a cada dia para fazer o SPAM que eles enviam chegar de maneira eficiente nos nossos endereços, ou seja, procurando burlar os nossos mecanismos de proteção contra o SPAM.

3.5. As técnicas SPAMMERS mais comuns nos dias de hoje

Vimos anteriormente que ocorreram fases na evolução do SPAM. Essas fases incluem os fatos ou técnicas mais marcantes que ocorreram em cada uma delas. Agora vamos falar sobre aquelas que são mais comuns nos dias de hoje.

OPEN RELAY (Relay Aberto): A técnica da utilização de máquinas com relay aberto foi muito explorada na chamada **2ª fase do SPAM** [6]. Esta técnica é menos utilizada hoje em dia, devido a uma melhoria nas configurações de muitos MTA, como o Sendmail [10], o Postfix [11], o Qmail [12], o Exim [13] e outros que, por default, impedem o relay (reenvio) indiscriminado de mensagens.

Porém ainda se verificam muitas máquinas com relay aberto, especialmente as que rodam o Microsoft Exchange, devido principalmente a imperícia daqueles que as administram. Sobre esse fato, da imperícia, ela pode ser verificada em lugares onde existam redes ligadas a Internet, mas onde a especialidade principal dos usuários e administradores não é nem a eletrônica nem a informática. Em tais redes, existem máquinas, algumas muito antigas, que são alvos freqüentes de "ataques" SPAMMERS.

WEB-SPAM: Já foi visto que na **3ª fase da evolução do SPAM** surgiu a técnica (de excelentes resultados) do WEB-SPAM. Mas o que é o WEB-SPAM?

Todos nos conhecemos as ferramentas de buscas na Internet (Astalavista, Yahoo e Lycos são os mais antigos, o Google é um mais recente e seguramente o melhor e mais popular deles). Mas muitos desconhecem como eles funcionam.

O funcionamento deles é bem simples. A partir das páginas já catalogadas no banco de dados, o **engenho de busca** (ou ***robot*** simplesmente) as re-visita periodicamente a procura de novos links para páginas novas, daí as páginas novas são adicionadas aos bancos de dados deles. É desta forma que se você tiver uma página não indexada e quiser adicioná-la aos engenhos de buscas, sem precisar entrar com cada um deles para fazer isso, bastará criar um link para ela numa página mais antiga, já indexada, que em questão de dias ela será adicionada aos bancos de dados dos engenhos de busca.

Mas o que isso tem haver com WEB-SPAM? Tudo! Imagine agora um engenho de busca que **vasculhe as portas 80** (HTTP) de quaisquer faixas de IP da Internet, periodicamente (um scanport mas apenas na porta 80), a procura de servidores HTTP instalados nas mesmas. Imagine que esse engenho de busca procure catalogar não as palavras-chaves da página mas **procure pela string "mailto" no código HTML**, que serve para abrir o cliente de E-mail da máquina visitante, quando o respectivo link for clicado. Se esse engenho de busca ler o conteúdo apontado pela tag MAILTO, ele poderá então catalogar esse endereço num banco de dados para SPAM.

Melhor ainda se, enquanto faz isso, o engenho de busca fizer queries DNS para encontrar o mail exchange do referido endereço de E-mail e enviar um ou mais SPAM para ele.

Esse engenho de busca existe em várias versões e essa técnica SPAM é conhecida como WEB-SPAM. É uma verdadeira praga que se estende até os dias de hoje por ser fácil, de baixo custo e difícil de ser barrada, principalmente porque é praticada a partir de máquinas que utilizam faixas de IPs temporários.

Observa-se que essa técnica de SPAM trouxe outro reflexo negativo, o aumento do trafego HTTP na Internet. Alguns meios eficientes de combate ao WEB-SPAM será mostrados mais adiante neste trabalho. É uma técnica muito usada em conjunto com o SPAM-SPOOFING.

SPAM-SPOOFING: Esta é **uma técnica mais moderna e bastante danosa** para o desempenho dos servidores SMTP de uma rede. Ela consiste em se conectar num servidor SMTP e, através de um engenho para gerar nomes comuns de contas de usuários (logins) de forma aleatória (ou fazendo uso de listas geradas elo WEB-SPAM), tentar enviar E-mails rapidamente e em grande quantidade.

Geralmente, por essa técnica, são feitas centenas ou até milhares de tentativas de envio de mensagens. O problema principal se deve ao fato que os endereços dos remetentes são geralmente falsificados. Dessa maneira e, principalmente, se o servidor SMTP for apenas um mail exchange, ele não terá como a priori saber se o nome do usuário de destino é verdadeiro ou não. Isto apenas ocorrera no servidor de destino da mensagem, o que provocara a rejeição da mesma, que voltará ao mail exchange, que tentará enviar para o mail exchange do suposto remetente, que provavelmente rejeitará a mensagem, que acabará na conta do postmaster do sistema da rede atacada pelo SPAMMER.

Observa-se que o trafego do SPAM foi multiplicado por um fator de 3 e este é o efeito danoso desta técnica SPAMMER, ela **aumenta a utilização da largura de banda do canal de comunicação externo de uma rede**.

SPYWARE: A técnica do **SPYWARE** (**4ª fase**), que **não teve origens SPAMMERS**, consiste em colocar-se uma tag HTML no cabeçalho de um SPAM. Dependendo do cliente de E-mail que o usuário estiver usando, ele fará acesso automático a uma determinada URL, que irá validar o endereço de E-mail num banco de dados, como um E-mail que o SPAM conseguiu atingir com sucesso.

A única forma de se evitar o SPYWARE é utilizando-se de programas de clientes de E-mail com suporte a HTML desativado, o que infelizmente desagrada a maioria dos usuários. Outra forma menos eficaz é tentar se localizar os servidores que recebem o SPYWARE e barrá-los na firewall.

FALSO LINK DE REMOÇÃO DE UMA LISTA SPAM: Técnica está que é bastante utilizada, semelhante ao SPYWARE, porém mais antiga (surgida na **3ª fase**). Consiste em adicionar um link HTML na mensagem eletrônica com um aviso que se o usuário deseja ser removido da referida lista de propaganda, basta **clicar no referido link**. Na verdade clicando em tal link, **o usuário estará confirmando que o E-mail dele é válido**, o que fará com que ele continue recebendo mais SPAMs ainda. Está técnica é muito **usada para enganar os usuários incautos ou novatos**.

Geralmente é adicionado um aviso (falso, lógico) que aquele E-mail está em complacência com um tal 105º Congresso Internacional de Bases Normativas sobre SPAM ou então que a constituição brasileira proíbe que E-mails sejam bloqueados (artigo constitucional da liberdade de expressão), etc. Tais mensagens são **embustes** para tentar intimidar os usuários ou administradores de redes incautos, com o intuito de amedrontá-los e desestimulá-los a colocar filtros de mensagens nos aplicativos de E-mails.

SPAM COM IMAGENS: Existem duas modalidades desta técnica (**3ª fase**), muito em voga atualmente: Com imagens anexadas ao E-mail e com código de HTML apontando para as imagens em um servidor remoto.

A primeira, por gerar E-mails muito grandes é geralmente evitada. A segunda, por gerar E-mail menores e ainda poder embutir SPYWAREs dentro do código HTML é mais utilizada.

A essência dessa técnica é evitar a análise do conteúdo de uma mensagem, pois não há atualmente softwares capazes de ler textos escritos dentro de imagens gráficas.

SPAM-ROUTING: Esta é uma das técnicas mais modernas de SPAM (**4ª fase**), é usada principalmente pelos **SPAMMERS profissionais**, pois é **muito cara de ser utilizada** e só o deve ser quando há perspectiva de um alto retorno financeiro dos SPAMs enviados.

O SPAM-ROUTING faz uso de várias linhas de conexão de Internet de alta velocidade, cada uma com uma máquina (servidor) SPAMMER dedicado, mas que estão interconectados por uma rede interna, também de alta velocidade. Há uma máquina que centraliza as operações, distribuindo as tarefas entre as demais.

No SPAM-ROUTING, quando uma máquina tenta enviar um SPAM e ele é rejeitado, a mesma retorna o SPAM e a mensagem de erro, do servidor SMTP que rejeitou a conexão, para a máquina centralizadora das operações. Está ira então repassar o SPAM para outra máquina da rede em outra conexão de alta velocidade, que tentará novamente enviar o SPAM por outro caminho.

O principio do SPAM-ROUTING é o de burlar as regras antispam que se baseiam em banir um E-mail proveniente de determinada faixa de IP ou de determinado domínio de um ISP. Nota-se que, para essa técnica ser eficiente, as conexões de alta velocidade devem ser constantemente trocadas (feito o rodízio), pois depois de algum tempo, a faixa de IP ou o domínio do ISP acaba ficando “sujos” na Internet.

O SPAM-ROUTING também faz uso do compartilhamento de recursos entre as redes de alta velocidade dos SPAMMERS profissionais de países diferentes. Neste caso quando um SPAM está sendo rejeitado por um servidor SMTP remoto, por quaisquer linhas de alta velocidade de uma determinada rede SPAMMER, esta roteia o SPAM através da Internet para o servidor de centralização de operações de outra rede SPAMMER em outro país, de onde provavelmente o SPAM terá mais sucesso de chegar ao seu destino. Igualmente válido para o SPAM-ROUTING será ter uma tabela atualizada de máquinas com relay aberto, que poderão também serem utilizadas para a operação de entrega das mensagens contendo SPAM.

Geralmente o SPAM-ROUTING que faz uso apenas de máquinas com relay aberto é utilizado por SPAMMERS não-profissionais ou com menores recursos financeiros, pois é bem menos caro de ser empregado e necessita de quantidades bem menores de linhas de conexão de Internet de alta velocidade.

4. Uma análise crítica sobre a legalidade do SPAM e os efeitos nocivos causados as redes na Internet e seus usuários pelas práticas SPAMMERS

Uma análise crítica sobre a legalidade ou não do SPAM é necessária num momento em que se começa, no Brasil e no mundo, a se discutir a criação de leis relativas aos chamados "crimes virtuais ou crimes na Internet".

A discussão é bastante extensa pois existem muitas dificuldades, inclusive como se caracterizar uma prova de crime existente apenas em formato digital e, portanto, facilmente fraudável.

Num primeiro momento poderíamos pensar que enviar E-mails com propaganda seria o equivalente a mala-direta postal que recebemos pelo correio de vez em quando (como já teve até juíza leiga no Brasil afirmando isso [44]). Mas analisemos os seguintes pontos:

- Numa mala-direta postal convencional, a pessoa ou entidade que a envia deve mandar imprimir o papel, comprar o envelope e pagar a taxa postal de envio.
- Numa "mala-direta" SPAM, a pessoa ou entidade que a envia paga apenas o preço da conexão que ela está usando do provedor de acesso. Desta forma os custos de envio desta são mais atrativos que o da mala-direta postal.
- As cartas da mala-direta postal nunca chegam ao número de milhares por mês (para alguns usuários) e geralmente não chegam num mesmo dia e nem entopem a caixa de correios das nossas casas ao ponto de não entrarem mais nada nela e caírem cartas para fora dela.
- A "mala-direta" SPAM pode chegar a milhares de mensagens por mês, o que significa **maiores gastos** homem/hora para ler, selecionar e apagar as mensagens. Alem disto, significa que os sistemas de correspondência eletrônica ficam mais sobrecarregados, o que acarreta mais acesso em disco pelos sistemas operacionais e a **necessidade de utilização cada vez maior de espaço em disco dos sistemas**, pois quase ninguém lê E-mails em tempo real. Em suma, isso significa **aumento de investimento e infra-estrutura de sistemas e redes** (ou seja, dinheiro) [8].
- Alem desses gastos, existe ainda um ônus a mais para várias redes de instituições publicas e privadas que é traduzido num **gasto maior da largura de banda do canal de comunicação externo** delas. A largura de banda do canal de comunicação externo (Bandwidth - Largura de Banda) não é grátis (como muitos pensam em lugares como a UFRJ), ela é paga e a taxação dela leva em consideração a utilização feita dela (para trafego entrando ou saindo da rede). Ou seja, o SPAM onera mais ainda as redes que o recebem.
- As mensagens de **SPAM** muitas vezes estão **associadas a atividades de fundo criminoso** tais como: Prostituição, pedofilia, venda de produtos proibidos pela legislação corrente de um país, contrabando, fraudes e golpes bastante lesivos as vítimas [8]. Conhece-se alguém que tenha recebido mala-direta postal de alguma prostituta?

- Alem de propaganda, os **SPAM podem transportar vírus/worms e/ou programas Trojans**, destinados a **coletar dados sensíveis dos usuários, tais como senhas, números de cartões de crédito ou bancários, números de CPF, números de contas bancárias, etc**. Fato que não acontece com a mala-direta postal convencional.

Analisando estes pontos colocados, chegamos a conclusão que o **SPAM é uma atividade que beneficia poucos em detrimento da maioria dos usuários da Internet**. Ele é uma pratica condenável porque **na pratica as redes e seus usuários são os que pagam o SPAM, quer comprem ou não os produtos ou serviços ali anunciados**.

O **SPAM se apropria de recursos dos sistemas das redes de terceiros** (largura de banda do canal de comunicação externo, espaço em disco e tempo de CPU) sendo portanto altamente lucrativo para que o pratica, pois em comparação a mala-direta postal, o custo da "mala-direta" SPAM é infinitamente menor.

A **médio e longo prazo**, se nada for feito para inibir as práticas SPAMMERS, **veremos os recursos da Internet sendo exauridos** por uma prática que não gera nenhum dividendo para a maioria dos usuários da Internet. Gera sim muito mais desperdício [5].

A **curto e médio prazo** a prática do SPAM está **corroendo a reputação da Internet Brasileira** [9], [16] e [38]. **Já existem listas mundiais que simplesmente banem todas as faixas de redes alocadas para instituições publicas ou privadas no Brasil**. Infelizmente tem-se notado de forma triste que aqui **no Brasil** [45] uma entidade ou **pessoa que pratica SPAM** é tratada como um **pobre coitado**, um **herói**, que está tentando conseguir uns trocados para alimentar os filhos. Por outro lado, **quem cria regras ou programas para banir mensagens de SPAM** é tratado como um **vilão que tenta impedir a liberdade de expressão das pessoas** livres e de bem.

Mudar tal mentalidade é difícil mas necessária, sob o risco de termos que fazer isso mais tarde já sobre a pressão de instituições publicas e privadas no exterior, e sob o risco de graves perdas de oportunidades econômicas devido ao desleixo como tratamos o problema do SPAM atualmente aqui no Brasil.

5. As técnicas ANTISPAM

As chamadas técnicas ANTISPAM surgiram quase ao mesmo tempo que os primeiros problemas relacionados as praticas de SPAM começaram a serem verificados. Tais técnicas não estão relacionadas a nenhuma RFC ou norma oficial, muito embora o desenvolvimento do SPAM tenha impulsionado uma melhoria nas RFC-821 e RFC-822, que se evoluíram para as RFC-2821 e RFC-2822, que introduziram formas de melhorar a identificação nos cabeçalhos das mensagens e de autenticação.

As **técnicas ANTISPAM destinaram-se a preencher as lacunas que a simplificação do protocolo SMTP deixou evidente** e que em muito acabaram facilitando o surgimento e o desenvolvimento das técnicas SPAMMERS.

Apesar de não terem um caráter ou uma norma oficial, as regras ANTISPAM existentes hoje surgiram como uma reação a cada nova modalidade de SPAM que surgia e são aceitas por grande maioria dos administradores e usuários de redes na Internet. Muitas delas podem ser implementadas dentro dos próprios servidores SMTP (MTA), através de bibliotecas em C/C++, ou a partir de plugins externos a eles, desta forma podem apresentar pequenas nuances entre diferentes servidores SMTP e plugins.

As regras ANTISPAM podem ser comparadas a três linhas de defesa que um SPAM deve tentar passar antes de chegar a um usuário final de uma rede. Podemos enumerar essas 3 linhas de defesa da seguinte forma:

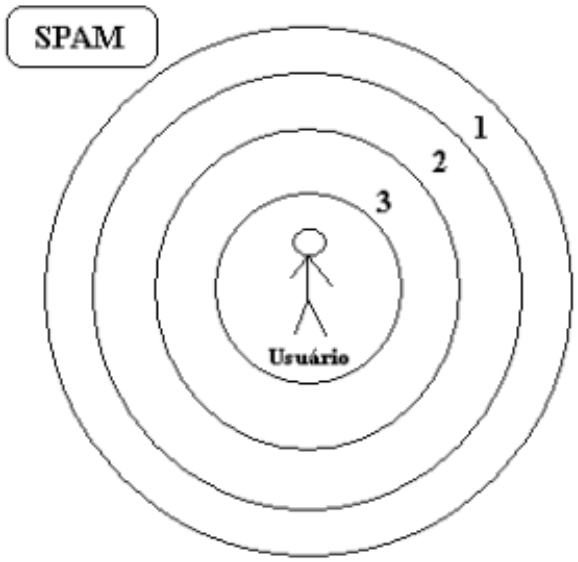

Fig.1 - As três linhas de defesa ANTISPAM

1. Regras, filtros internos ou técnicas ANTISPAM que são implementadas dentro do código-fonte do servidor SMTP, podendo ou não usar bibliotecas externas C/C++, com as implementações de tais técnicas, que são adicionadas ao código binário resultante durante a compilação do código executável.

2. Uso de plugins (programas externos) que não são compilados dentro do servidor SMTP, mas são aplicativos separados rodando em paralelo e interconectando-se com o mesmo.
3. Uso de programas ANTISPAM a nível do próprio usuário, que é o destinatário final da mensagem.

As regras ou técnicas da **1ª linha de defesa** tem por função tentar **resguardar a largura de banda do canal de comunicação externo da rede e os recursos do sistema, alem do usuário final**, tentando para isso se antecipar em deduzir se uma mensagem pode ser um SPAM ou não. O uso de programas plugins externos a nível do servidor SMTP, que são a **2ª linha de defesa**, destinam-se a **resguardar os recursos do sistema** (disco, tempo de CPU e/ou custo homem/hora para ler e apagar mensagens de SPAM) e o usuário final. Por fim, os próprios programas ANTISPAM a nível de usuário, a **3ª linha de defesa**, procuram **resguardar o usuário em si** da situação inconveniente causada pelo recebimento de SPAMs.

Antes de começarmos a discorrer sobre cada modalidade de técnicas ANTISPAM, devemos analisar sucintamente como funcionavam os servidores SMTP antes e depois do fenômeno do SPAM surgir para podermos ter uma boa idéia de como tal fenômeno provocou uma mudança radical de se tratar comunicações SMTP na Internet.

Após isto, trataremos das técnicas ANTISPAM propriamente ditas, primeiro a nível da administração de redes e depois a nível dos usuários de redes.

5.1. Os servidores SMTP (MTA) antes e depois do SPAM

Até o **início de 1996** já existiam bastantes **servidores SMTP** funcionando na Internet, **a sua imensa maioria rodando Sendmail**, existindo outros como o **Smail** do Linux e o **Mercury** das Novell Netware (embora esse último recebesse conexões SMTP, ele **necessitava do Sendmail ou do Smail de um Unix como host-relay** para enviar os E-mails). O Sendmail ainda continua sendo o mais utilizado nos dias de hoje devido a sua grande portabilidade para diversos tipos de sistemas operacionais diferentes, especialmente os chamados "Unix-like" (Linux, FreeBSD, etc). Atualmente se encontra em desenvolvimento a versão alpha do novo Sendmail-X, que inclui conceitos de modularização em suas funcionalidades.

Tais servidores SMTP funcionavam baseados no protocolo SMTP como descrito na RFC-821datada de 1981 e as características deles eram as seguintes:

- Funcionavam seguindo o **protocolo SMTP** da **RFC-821**, **sem restrições**;
- Possuíam **relay aberto por default**, ou seja, aceitavam receber e fazer relay de E-mails de quaisquer origens para quaisquer destinos;
- **Praticamente** não possuíam **nenhuma regra de filtragem** para conexões SMTP, quando muito limitavam o tamanho total de uma mensagem;
- Não possuíam possibilidade de funcionamento com plugins de terceiros;
- Alguns eram Open-Source, como o Sendmail e o Smail, outros como o Mercury eram proprietários;
- Não possuíam a habilidade de fazer autenticação para permitir relay de mensagens;
- Apesar de não serem bem projetados, **trabalhavam bem porque o trafego de E-mails não era pesado**, não exigindo processamento excessivo.
- Eram **mais difíceis de serem configurados, especialmente o Sendmail**, o que fatalmente não incentivava os administradores de redes a alterarem as configurações defaults.

Após a primeira metade de 1997, já na da 2ª fase do SPAM, quando as máquinas com relay aberto começaram a serem exploradas para o reenvio das mensagens de SPAM, várias características foram alteradas nos servidores SMTP para cobrirem as "fragilidades" do protocolo SMTP, que foram as seguintes:

- Passaram a funcionar **ainda seguindo o protocolo SMTP da RFC-821** (e **posteriormente da RFC-2821**), **agora fazendo restrições** porém respeitando a norma do protocolo SMTP (utilizando os códigos de errors e avisos da mesma);
- Passaram a trabalhar com **relay fechado por default**, ou seja, faziam algumas verificações de IP ou domínio da máquina de origem antes de permitir ou não o relay de uma mensagem;
- Passaram a fazer **filtragem das mensagens de diversas formas**, de forma a identificar se as mesmas era ou não SPAM de forma razoável;

- Passaram a **permitir o funcionamento com plugins de anti-virús e anti-spam** de terceiros;
- Surgiram **novos servidores SMTP Open-Source** como o **Postfix**, o **Qmail** e o **Exim** (atualmente a maioria dos servidores SMTP são de código-aberto), e **outros proprietários, como o Microsoft Exchange** (que até hoje é o mais deficiente, provavelmente por falta de habilidade dos administradores de redes em configurá-lo, para evitar SPAM). As redes **Novell Netware sofreram grande recuo no mercado** e com isso a **utilização do Mercury diminuiu**;
- Passaram a **permitir a possibilidade do uso de autenticação** para permitir relay de mensagens;
- Passaram a ser **projetados melhor para poderem trabalhar com mais eficiência** devido ao SPAM tornar o trafego de E-mails consideravelmente pesado, exigindo um processamento maior.
- Passaram a serem **mais fáceis de serem configurados**, com uma **melhor documentação das configurações**, o que facilitou e incentivou os administradores a fazerem configurações personalizadas para cada realidade de rede diferente.

Como pode ser notado, praticamente **houve uma mudança de 180º na mentalidade da construção e da operação dos servidores SMTP**. Claro que tal mudança não seria bastante para conter os problemas relacionados com SPAM, desta forma, foram sendo criadas técnicas extras chamadas de técnicas ANTISPAM, que aos poucos passaram a ser aceitas de formas mais ou menos homogêneas.

5.2. Técnicas ANTISPAM em nível de administração de redes

As **primeiras técnicas ANTISPAM** surgiram em **nível de administração de redes**, especialmente porque não existiam softwares ou plugins que permitissem aos usuários terem regras individualizadas para a prevenção de SPAM.

Como **tais regras são globais**, ou seja, **afetam invariavelmente TODOS os usuários de uma rede**, elas devem ser elaboradas e aplicadas com o máximo cuidado possível de forma a bloquear a maior quantidade de SPAM possível e reduzir ao mínimo o risco dos chamados casos de "falso positivo" para SPAM.

A seguir descreveremos as principais técnicas ANTISPAM em nível de administração de redes, ou seja, configuradas diretamente ou via configuração de plugin, em um servidor SMTP, discorrendo sobre suas vantagens e desvantagens.

Dos tópicos abaixo discorridos, os que vão de 5.2.1 até 5.2.6 são referentes a chamada 1ª linha de defesa contra SPAM. A analise dos conteúdo de E-mails pelo servidor SMTP usando plugin, em 5.2.7, é referente a chamada 2ª linha de defesa contra SPAM.

5.2.1. Regras de filtragem interna dos servidores SMTP

As regras de filtragem interna dos servidores SMTP (MTA) são geralmente bastante básicas e **remontam a época da 2ª fase do SPAM**, quando os servidores SMTP começaram a serem modificados pelos próprios desenvolvedores para se fazer frente as práticas SPAMMERS mais básicas.

Em geral são regras bastante simples e fáceis de serem configuradas:

- Bloqueio de mensagens oriundas de um numero IP ou de uma faixa de números IP;
  Exemplo: 192.168.0.0/24 REJECT
- Bloqueio de mensagens oriundas de um determinado FQDN (Fully Qualified Domain Name);
  Exemplo: sexhot.com REJECT
- Bloqueio de mensagens oriundas de domínios inexistentes;
  Exemplo: MAIL FROM: diabo@wsjdhgstevsrftrs.uuu
  550 5.7.1 Rejected. Invalid domain wsjdhgstevsrftrs.uuu
- Bloqueio de mensagens com domínio inexistente ou inconsistente quando do comando SMTP HELO (OBS.: Pouco utilizada devido ao fato do comando HELO ser costumeiramente preenchido com informações sem consistência nenhuma);
  Exemplo: HELO wsjdhgstevsrftrs.uuu
  550 5.7.1 Rejected. Bad domain in HELO
- Mensagens oriundas de um determinado endereço;
  Exemplo: MAIL FROM: ocarteiro@correio.com.br
  550 5.7.1 Rejected. Bad remote user address
- Bloqueio de mensagens para um determinado usuário local;
  Exemplo: RCPT TO: local-list@mydomain.com
  550 5.7.1 Rejected. Local user don't receive messages

- Relay incondicional de mensagens restrito a rede local;

Exemplo: 146.164.48.0/26 RELAY
ALL REJECT

5.2.2. O uso das BlackLists

A **técnica da BlackList** ou **RBL** (**Realtime Black List**) ou mais modernamente **DNSBL** (**Domain Name Service Black List**) é uma técnica ANTISPAM surgida na época da **2ª Fase do SPAM**, quando eram mais exploradas as máquinas com relay aberto.

Esta técnica foi **concebida por Paul Vixie**, que mais tarde fundaria uma entidade chamada de **MAPS** (**Mail Abuse Prevention System**) [2], que teve o brilhantismo de utilizar a própria base instalada dos servidores de **DNS** (**Domain Name Service**) [26] e [27] mundiais para propagar a informação das BlackLists por ele criada.

Mas como funciona em si a técnica da BlackLists ou DNSBL? Existem alguns sites na Internet que explicam de forma mais detalhada esta técnica, um deles é o site da ANTISPAM-UFRJ [15], de onde se baseou a explicação desta técnica.

Supondo que, por algum método, uma entidade mapeou servidores de SPAMMERS, servidores SMTP com relay aberto e/ou faixas de IPs temporários e queira disponibilizar essa informação pela Internet, ela pode fazer uso de uma tabela de DNS direto de um subdomínio dela.

Vamos tomar de exemplo a base de dados de relay aberto, supondo que a entidade se chama **antispam.foo**, ela cria um subdomínio chamado **open-relays.antispam.foo**. Neste subdomínio ela indexará os IPs 10.0.0.1, 10.0.0.5, 10.0.0.7 e 10.0.0.15. Para indexá-los, ela simplesmente **coloca os octetos na ordem reversa** e **acrescenta o subdomínio neles, apontado-os para um IP da classe A 127.0.0.0/8**, com **exceção do 127.0.0.1** (LoopBack IPv4). Abaixo um fragmento de tabela de DNS exemplifica o que foi aqui escrito:

1.0.0.10.open-relays.antispam.foo	IN	A	127.0.0.2
5.0.0.10.open-relays.antispam.foo	IN	A	127.0.0.2
7.0.0.10.open-relays.antispam.foo	IN	A	127.0.0.2
15.0.0.10.open-relays.antispam.foo	IN	A	127.0.0.2

Suponhamos agora que um servidor SMTP consulta a BlackList de relays abertos da antispam.foo. Neste servidor deverá ter configurado a lista a ser consultada, que no caso se traduz pelo subdomínio open-relays.antispam.foo.

Se a máquina 10.0.0.5 conectar neste servidor SMTP, o mesmo fará uma consulta ao DNS da rede dele **para saber qual o IP** de **5.0.0.10.open-relays.antispam.foo**. Obviamente o **IP será 127.0.0.2**, o que **indica que a máquina 10.0.0.5 está na tabela de máquinas com servidor SMTP com relay aberto**, e o servidor SMTP deve retornar uma mensagem de erro explicativa e **terminar a conexão SMTP sem que a mensagem vinda daquela máquina seja recebida**.

Como se pode ver o funcionamento e a consulta de um DNSBL é muito simples. Devido a isso é que existem milhares de redes em todo o mundo que fazem consultas as várias entidades mundiais que mantém DNSBLs ativos. Dentre estas entidades, as que

mantêm as listas mais famosas (e mais consultadas) são o MAPS-RBL [2], o SpamCop [7] e o SpamHaus [4].

Os DNSBLs são bastante práticos, porém um problema relativo a eles é derivado do fato que a consulta a eles é através dos mecanismos de resolução de nomes, que utiliza o protocolo UDP, ou seja, não há garantia do retorno da solicitação da consulta.

Isto gera o problema dos "falsos negativos" em redes com conexões externas lentas ou quando se consulta listas com poucos servidores DNS secundários. Por "falso negativo" entenda-se o fato da consulta ser feita e não haver resposta, geralmente neste caso é retornado um host not found ou host unknow, o que para o mecanismo de BlackList significa que a máquina não esta indexada na lista consultada, mesmo que esteja, e neste caso um SPAM poderá passar livremente até o seu destinatário.

Para diminuir a possibilidade de "falsos negativos", as entidades que mantêm DNSBLs costumam ter alguns DNS secundários "espalhados" na Internet, o que previne da informação não estar disponível por quaisquer motivos de queda em suas conexões externas com a Internet.

Outra forma de diminuir a ocorrência de "falsos negativos" e o servidor SMTP fazer consultas a mais de uma entidade, partindo do pressuposto que a máquina SPAMMER possa estar indexada em mais de uma lista, porém consultar um número grande de BlackLists pode diminuir sensivelmente a performance do mesmo.

5.2.3. O uso da técnica de GrayListing

A técnica de **GrayListing** [17] é uma **técnica relativamente recente**, surgiu por volta de 2001, é baseia-se em fazer uma lista de bloqueios temporários em tempo real. Ela foi criada para combater em maior grau o SPAM-SPOOFING e em grau intermediário o WEB-SPAM e o SPAM-ROUTING, sendo porém aplicada a outras modalidades de SPAM.

O princípio de funcionamento do GrayListing é o de rejeitar a primeira conexão de um cliente remoto e esperar um determinado tempo antes de liberar o recebimento da mensagem na conexão seguinte.

Suponhamos que a máquina 192.168.0.2 conecte em um servidor SMTP que esta configurado para utilizar a técnica da GrayListing. Supondo ser a primeira conexão dela para enviar aquela determinada mensagem, o servidor SMTP irá copiar numa lista o número IP da máquina remota, o remetente passado no comando SMTP **MAIL FROM** e o destinatário passando no comando SMTP **RCPT TO**. Imediatamente após isso, ele retorna uma mensagem SMTP com o código de erro temporário (451 4.1.8), o que instrui o cliente (se ele for um servidor SMTP) a tentar conectar novamente mais tarde (tipicamente 1 minuto) e encerra a conexão.

A idéia do uso do GrayListing é que os SPAMMERS usam engenhos (**robots**) para enviar SPAMs e não servidores SMTP normais, pois não querem receber avisos de erros e nem reclamações por SPAMs por eles enviados e querem enviar o maior número de mensagens o mais rapidamente possível. Geralmente esses **robots são programas muito simples e rústicos**, sendo que **enviam E-mails de forma seqüencial e não gerenciam filas de saída**, para serem bastante rápidos. Logo, a possibilidade do robots

tentar enviar novamente o SPAM será pequena, pois muitas vezes eles tem que enviar milhares ou milhões de E-mails, o que leva horas ou até dias.

Desta forma, após passado um certo tempo (um 1 minuto), se a máquina 192.168.0.2 conectar novamente, provavelmente estará rodando um servidor SMTP e a possibilidade da mensagem ser um SPAM será menor. Assim, a entrada relativa aquele E-mail inicialmente rejeitado será removida da GrayListing do sistema e a mensagem poderá ser entregue.

A técnica do **GrayListing foi muito eficaz quando foi lançada**, e muitos achavam que isso iria ser eternamente eficaz contra o SPAM. Infelizmente tem-se observado nos últimos tempos que novos tipos de robots SPAM estão trabalhando com gerenciamento de filas e listas menores, para tentarem assim poderem burlar a técnica da GrayListing.

Um outro problema que se tem notado com GrayListing é quando um pessoa envia vários E-mails para outra cujo servidor SMTP implemente GrayListing. O tempo de espera imposto pelo servidor SMTP pode fazer com que as mensagens cheguem ao destinatário fora de ordem, caso o usuário esteja lendo as mensagens num horário próximo ao do envios das mensagens.

Há ainda o fato que alguns poucos ISP, por terem trafego de E-mails muito elevados ou por inexperiência de seus administradores de rede, costumam programar seus servidores SMTP para retornarem as mensagens para os usuários após quaisquer erros (mesmo que temporários) sem tentar reenviá-las, logo após a primeira tentativa.

5.2.4. A regra da verificação da consistência do DNS reverso (RFC-1912)

A técnica da **consistência do DNS reverso** [39] e [40] tem por base **interpretar ao pé da letra a RFC-1912** [28]. Esta RFC informativa instrui que **quando um FQDN é atribuído a um número IP no DNS, este numero IP deve apontar para esse FQDN no DNS reverso**, independentemente de existirem ou não outros FQDNs apontando para esse mesmo numero IP. **Está técnica ANTISPAM é** considerada **uma das mais agressivas**.

Desta forma, **está técnica pressupõem** que a **maioria dos SPAMMERS preferem tacitamente o anonimato** e assim eles preferirão usar as faixas de IPs dinâmicos de ISPs que, por comodidade ou ignorância dos administradores de redes dos ISP, não sigam o que esta escrito na RFC-1912. Na verdade, **poucos ISPs configuram DNS reverso** para as próprias faixas de IPs dinâmicos e quando o fazem, geralmente o fazem com denominações bem sugestivas com ppp, dialup, users, etc, para a comodidade deles.

Da mesma forma, **os SPAMMERS** que possuem linhas dedicadas tipo ADSL **não fazem nenhuma questão de pedir aos ISPs que estes apontem corretamente o DNS reverso do número IP**, que eles estão usando na linha dedicada, para o nome do domínio na Internet da pessoa jurídica (empresa) que eles, os SPAMMERS, utilizam para dar suporte as atividades SPAMMERS que eles praticam.

Realmente, já se verificou em muitas ocasiões que a **maior parte dos SPAM recebidos por muitos usuários provêem de IPs sem DNS reverso ou com DNS**

reverso inconsistente, o que significa, neste último caso, que o IP aponta para um FQDN que não aponta de volta para esse mesmo IP.

O **ponto fraco** desta técnica de verificação de consistência do DNS reverso é que **a possibilidade de ocorrerem os chamados "falso positivos" não é desprezível**, principalmente porque existem administradores de rede desleixados ou ignorantes que não configuram o DNS reverso para os servidores SMTP das suas respectivas redes. Muitos deles **ficam até insistindo que a configuração das suas redes estão perfeitas** e que eles **não irão modificar nada nelas**, numa total **demonstração de ignorância das normas requeridas para o bom funcionamento da Internet**.

É recomendável, porém, o uso desta técnica quando a quantidade de SPAMs recebidos semanalmente por um usuário for grande, pois fatalmente o endereço do dele já devera estar indexado em centenas ou até milhares de listas SPAMMERS de todo o mundo. Porém é recomendável **deixar esse tipo de decisão nas mãos do próprio usuário e não por conta apenas do administrador da rede**, para se evitar possíveis atritos entre ambos

5.2.5. A regra da verificação das strings do DNS reverso

Está **técnica é semelhante a anterior**, porém ela **se baseia apenas em verificar, caso o DNS reverso do IP da maquina remota esteja configurado, as strings que compõem o FQDN apontado pelo DNS reverso**. **Está técnica ANTISPAM é** também considerada **uma das mais agressivas**, tal qual a anterior.

A idéia desta técnica é procurar achar strings (cadeias de caracteres) típicas que identifiquem o tipo de conexão usada pela maquina remota e supor se á máquina está usando um IP temporário ou uma conexão dedicada de IP fixo e, neste último caso, se a máquina com IP fixo é uma máquina que pode enviar E-mails de SPAMs ou não.

Já se verificou, como na técnica anterior, que grande parte dos SPAMs também vem de maquinas cujos números IPs apontam para FQDN com strings típicas de conexões de IPs temporários, como ppp, dial, dialup, users, dip, etc.

Também usa-se essa técnica para partir do principio que, **se uma empresa séria compra uma conexão dedicada e quer enviar E-mails seriamente e não como SPAMMERS, ela irá exigir que o DNS reverso do ISP aponte para o FQDN dela**.

Exemplo:

Fragmento de tabela de DNS direto:

mail.minhaempresa.com IN A 192.168.254.8

Fragmento de tabela de DNS reverso:

8.254.168.192 IN PTR mail.minhaempresa.com

Caso o contrario, **sendo uma empresa que trabalha com E-mail marketing** (ou seja, SPAM), ela **ira querer anonimato e não ser identificada com facilidade** por quem recebe o SPAM, **logo não irá exigir nada disso ao ISP**.

O **ponto fraco** dessa técnica é que **algumas empresas**, geralmente por **desconhecimento ou ignorância das RFC pelos seus administradores de rede**, não fazem nada disso. **Logo a ocorrência de "falsos positivos" nesta técnica também não poderá ser considerada desprezível**.

Tal qual a regra anterior, está é recomendável quando a quantidade de SPAM recebidos por um usuário diariamente é muito elevada, pois ele possivelmente esta indexado em centenas ou milhares de listas SPAMMERS. De todo modo, **a decisão de fazer-se isso ou não deve se deixada por conta do próprio usuário**, também para evitar atritos desnecessários com o administrador de redes.

Apesar da agressividade dessas duas regras ANTISPAM, já verificou-se que, **na pratica, é com o uso de ambas que se consegue barrar a maior parte do SPAM atualmente**, pois usando-se elas os SPAMMERS, que em sua imensa maioria são covardes atrás de um computador, tem de escolher entre continuar não conseguindo enviar os E-mails de SPAM ou terem que identificar corretamente os números IP nos DNS direto e reverso de suas redes e correrem o risco de serem identificados e de terem os respectivos domínios na Internet colocados em listas negras, alem de outras sanções penais poderem ser-lhes imputadas mais facilmente.

5.2.6. Verificação da consistência do comando MAIL FROM

A técnica da verificação da consistência do comando SMTP **MAIL FROM** é uma técnica surgida durante a **3ª fase do SPAM**.

Esta técnica **pressupõem que o SPAMMER procurara na maioria das vezes mascarar sua identidade** colocando um endereço inconsistente durante o comando SMTP **MAIL FROM**.

Uma verificação de consistência já é feita atualmente pelos servidores SMTP, que checam se o domínio do endereço passado no comando SMTP **MAIL FROM** é válido. Isto foi implementado primeiro no Sendmail no final da 3ª fase dos SPAM, pois verificou-se que a maioria dos SPAMs na época colocavam domínios inexistentes nos endereços passados durante do comando SMTP **MAIL FROM**. Eles faziam isso para que o E-mail não tivesse retorno e acabassem parando o endereço do postmaster do sistema.

Infelizmente **essa verificação logo foi burlada**, passando-se a colocar no comando SMTP **MAIL FROM** endereços validos, na maioria dos caso, ou aos menos com domínios existentes, o que acabou acarretando que, fatalmente, algum postmaster iria acabar recebendo o SPAM que havia sido enviado, o que só fez aumentar o trafego SMTP, ao invés de diminuí-lo.

Alem da verificação de consistência acima, outras três podem ser feitas: O uso do null-reverse path (<>), o uso do domínio local, a verificação de "caracteres proibidos" e a verificação se o servidor remoto aceita receber conexões SMTP.

Verificação do null-reverse path: O uso do null-reverse path (quando se coloca <> após o comando SMTP **MAIL FROM**) é previsto desde a RFC-821 (atualmente RFC-2821). Ele foi criado como uma forma do próprio servidor SMTP enviar E-mails de erros ou avisos evitando a ocorrência dos chamados mails-loops. Um mail-loop pode ser gerado em condições especiais, por exemplo, por um alias mal configurado, que provoque que o mesmo E-mail passe continuamente pelo servidor SMTP (como se você andasse em círculos) infinitas vezes. Antigamente isso provocava um uso excessivo da CPU pelo servidor SMTP, provocando muitas vezes a queda do sistema. Atualmente os servidores SMTP possuem artifícios mais ou menos eficazes para evitar o mail-loop infinito.

Porém, a **RFC-821 não restringiu o uso do null-reverse path apenas ao servidor SMTP da rede local**. Devido a isso, **ele se tornou muito prático para os SPAMMERS e para os criadores de vírus**, pois o servidor SMTP muitas vezes mascara o null-reverse path com o nome MAILER-DAEMON, e o usuário incauto pensa tratar-se de um E-mail de erro do sistema e o abre pensando tratar-se de algo muito importante.

Restringir-se o uso do null-reverse path apenas a rede local e as "redes amigas" é uma excelente pratica que evita uma boa quantidade dos SPAMs que se receberia normalmente.

Verificação do uso do domínio local: Consiste em permitir que **somente as máquinas da rede local e de "redes amigas" possam colocar um endereço com o domínio da própria rede local** durante o comando SMTP **MAIL FROM**. Muitos SPAMs são geralmente recebidos contendo a informação que ele veio a partir do próprio endereço do usuário ou de outros usuários da rede, de forma a tentar enganar o usuário local que queira descobrir como isso aconteceu.

Apesar de ser uma **boa prática fazer esse tipo de restrição**, ela tem o **inconveniente que o usuário não poderá mais enviar E-mails para outros endereços na rede local, contendo como endereço de origem o seu próprio endereço na rede local, a partir de outras redes que não sejam a própria rede local ou as "rede amiga"**.

Exemplificando: Se a rede local é 10.0.0.0/24, com domínio foo.org, e ele quiser enviar um E-mail a partir de 192.168.0.0/24, usando no comando SMTP **MAIL FROM** o endereço dele, por exemplo ele@fog.org. Se a rede 192.168.0.0/24 não for configurada como "rede amiga" no servidor SMTP da rede 10.0.0.0/24, a conexão SMTP será rejeitada.

Verificação de caracteres "proibidos": Consiste em rejeitar conexões SMTP quando, durante o comando SMTP **MAIL FROM**, o endereço passado contiver caracteres considerados "proibidos". Entende-se por isto caracteres não usuais em endereços SMTP passados no comando SMTP **MAIL FROM**, como &, #, !, ~, _, (,), ^, *, etc. Uma **grande parte dos SPAMs possuem caracteres "proibidos"** para mascarar ainda mais a identidade do remetente. Robots também costumam usar esses caracteres no gerador de nomes aleatórios de usuários.

O **problema desta verificação** é que **vários ISP permitem o uso de alguns caracteres que seriam considerados "proibidos"**, tais como o _ e o & (os mais utilizados pelos SPAMMERS) nos endereços de origem das mensagens de seus usuários.

Verificação se o servidor remoto aceita conexão SMTP: É realizada por alguns servidores SMTP como o Postfix (mas não como configuração default) após o comando SMTP **MAIL FROM**. Eles verificam se a máquina que fez a conexão aceita receber conexões SMTP (principio da bi-direcionalidade).

O **problema principal** desta técnica é que **muitos ISP costumam configurar os chamados MAILHUBS**, que são máquinas que apenas enviam E-mails de dentro para fora da rede, e os MAILHOSTS, que são máquinas que só recebem conexões de dentro para fora da rede. Logo a possibilidade de "falsos positivos" é alta. Alem disso, existe o tempo de delay que é criado para liberar ou não a mensagem, que no pior caso será o tempo de timeout da conexão SMTP para o servidor remoto.

5.2.7. Análise do conteúdo de E-mails pelo servidor SMTP usando plugin

O uso de plugins nos servidores SMTP está muito em voga atualmente. Alguns plugins são para a prevenção de E-mails contendo vírus, outros para a prevenção de SPAMs.

Para a prevenção de SPAM, alguns plugins como o Spam-Assassin [41], oferecem suporte a análise do conteúdo de um E-mail, geralmente pelo método da pontuação, que será descrito mais adiante, pois ela pode também ser utilizada por programas próprios dos usuários.

Existem três problemas relacionados com o uso de plugins para a analise do conteúdo de E-mails para a verificação da ocorrência de SPAM:

1. Eles **não impedem a degradação da largura de banda do canal de conexão externo das redes**, pois tem que receber toda a mensagem para analisá-la.
2. **Dependendo da configuração** feita pelo administrador da rede, eles **não impedem o usuário de receber o SPAM**, apenas colocam um aviso no subject (título) da mensagem avisando que provavelmente se tratar de um SPAM, ficando a análise final do conteúdo e a remoção do E-mail por conta do destinatário final da mensagem. **Desta forma os problemas ao sistema, causado pelo acumulo de mensagens inúteis, continuam**.
3. Atualmente eles são ineficazes para verificar SPAMs que se valem da técnica do **SPAM COM IMAGENS**, o que será visto mais adiante também.

Por isso, o **uso de plugins para combate a SPAM deve ser encarado como uma ferramenta auxiliar as regras ANTISPAM** vistas anteriormente, ou seja como uma 2ª linha de defesa contra SPAM, e não como única alternativa para elas.

5.2.8. Comentários sobre uma técnica "nati-morta", o MARID

O **MARID** (**MTA Authorization Record in DNS**) [29] era uma técnica de autorização com certificação proposta pela Microsoft, no início de 2004, junto a IETF e que faria uso da base instalada de servidores DNS (tal qual a técnica da BlackLists, porém através da resolução de uma entrada nova na tabela do DNS, que seria adicionada por uma nova RFC específica) para a certificação digital de servidores SMTP, com intuito de combater o SPAM. Essa técnica, **se tivesse vingado**, seria mais uma técnica da chamada **1ª linha de defesa contra SPAM**.

Era a essa técnica inclusive que o fundador da Microsoft, **Bill Gates**, se referiu bastante no ano de 2004 quando **afirmou que o SPAM duraria no máximo mais dois anos**.

Nesta técnica, o servidor SMTP, ao receber uma conexão remota, poderia receber ou não um certificado (o uso desta técnica de certificação não seria obrigatório, para se manter a compatibilidade com os sistemas mais antigos).

Se recebesse o certificado, ele procuraria autenticá-lo fazendo uma resolução de DNS. Caso a autenticação fosse confirmada, ele permitiria a passagem da mensagem sem a necessidade de verificação de quaisquer regras ANTISPAM, pois a autoridade certificadora garantiria que o cliente remoto não é um SPAMMER.

Embora na teoria essa técnica parecesse boa, algumas indagações ficam. Quem seria a autoridade certificadora? Como seriam os certificados? Quanto custariam? Qual seria o tempo de validade dos certificados? Como saber se um SPAMMER não iria adquirir um certificado? (Lembrando-se que se pressupõem que a atividade SPAM seja altamente lucrativa, por que os SPAMMERS não comprariam certificados).

Infelizmente essas questões ficarão sem respostas, pois **o IETF descontinuou o desenvolvimento do MARID** [30] ainda no final de 2004 **devido a exigências relativas a patentes feitas pela Microsoft a IETF** [31], ou seja, a Microsoft "vendeu" a idéia do MARID para o IETF, que trabalhou muito para fazê-lo um padrão aberto e sem pagamento de patentes, e depois, no meio do caminho, "mudou" de idéia. Assim, o MARID acabou sendo abandonado pela IETF, que não queria impor um padrão de certificação, num protocolo aberto, que implicaria no pagamento de direitos de patentes para terceiros.

O MARID está sendo aqui citado porque, alem do ter sido bastante comentado no passado recente, ele foi a primeira tentativa de se introduzir certificação na troca de mensagens eletrônicas. Infelizmente não foi adiante e por enquanto ainda não há uma nova proposta satisfatória para certificação na troca de mensagens eletrônicas.

5.3. Técnicas ANTISPAM em nível de usuários de redes

As técnicas ANTISPAM em nível de usuários de rede são aquelas implementadas a nível das aplicações que os usuários utilizam para ler seus E-mails ou, de modo mais geral, a nível de programas auxiliares externos (plugins) para tais aplicações.

Tais técnicas começaram a surgir no final da **3ª fase do SPAM** e constituem-se na **3ª linha de defesa** antes de um SPAM conseguir alcançar um usuário, muito embora na verdade o SPAM chegue na caixa de entradas do usuário, pois o aplicativo apenas irá marcar a mensagem como um SPAM ou irá mover a mensagem para uma caixa de mensagens especial para o usuário posteriormente examinar ou apagar sem ler nada.

Nota-se que **ao chegar neste ponto**, o **SPAM já prejudicou a largura de banda do canal de comunicação externo da rede e os recursos do sistema** (disco e tempo de CPU). Dependendo da situação, **poderá ou não afetar ainda o custo homem/hora** para ler ou não as mensagens e apagá-las.

O tópico 5.3.5, cuidados especiais para evitar de entrar em listas de SPAMMERS, discorre sobre conselhos importantes para evitar que um endereço eletrônico seja indexado em listas de SPAMMERS. Tais conselhos ajudarão em muito em evitar que a quantidade de SPAMs recebidos cheguem a níveis insuportáveis.

5.3.1. A análise dos cabeçalhos das mensagens

A técnica de análise dos cabeçalhos de uma mensagem consiste em verificar os campos principais que formam a parte da mensagem responsável pela identificação do remetente (From:), do destinatário (To:), o assunto da mensagem (Subject:), os servidores SMTP por onde a mensagem passou antes de chegar em seu destino (campos Received:), etc. Os campos dos cabeçalhos de uma mensagem foram descritos inicialmente na RFC-753 (1979), RFC-822 (1981) e atualmente são descritos pela RFC-2822 (2001). Abaixo segue um exemplo típico de um cabeçalho de um E-mail SPAM originado de uma máquina com um servidor SMTP bem arcaico e possivelmente aberto (**relay aberto** ou **open relay**):

```
From root@sd.znet.com Fri Jun 15 15:00:38 2001
Received: from sd.znet.com (sd.znet.com [207.167.64.5])
     by mx3.znet.com (8.11.4/8.11.4/jjb-mx3) with ESMTP id f5FM0bU29917
     (using TLSv1/SSLv3 with cipher EDH-RSA-DES-CBC3-SHA (168 bits) verified
NO)
     for <spam@mx3.znet.com>; Fri, 15 Jun 2001 15:00:38 -0700 (PDT)
Received: (from root@localhost)
     by sd.znet.com (8.11.4/8.11.4/jjb-sd) id f5FM0ZP18260
     for spam@mx3.znet.com; Fri, 15 Jun 2001 15:00:35 -0700 (PDT)
Received: from mx1.znet.com (mx1.znet.com [207.167.64.1])
     by sd.znet.com (8.11.4/8.11.4/jjb-sd) with ESMTP id f5FM0Xc18245
     (using TLSv1/SSLv3 with cipher EDH-RSA-DES-CBC3-SHA (168 bits) verified
NO)
     for <mitchm@sd.znet.com>; Fri, 15 Jun 2001 15:00:34 -0700 (PDT)
 Received: from dec1.peq.coppe.ufrj.br (dec1.peq.coppe.ufrj.br [146.164.51.97])
      by mx1.znet.com (8.11.4/8.11.4/jjb-mx1) with SMTP id f5FM0V918160
      for <mitchm@lapcopaintball.com>; Fri, 15 Jun 2001 15:00:33 -0700 (PDT)
 X-Envelope-From: F17753@earthlink.net
 X-Envelope-To: <mitchm@lapcopaintball.com>
```

```
 Received: by dec1.peq.coppe.ufrj.br; id AA03455; Fri, 15 Jun 2001 21:00:46 -
0300
 Message-Id: <10106160000.AA03455@dec1.peq.coppe.ufrj.br>
 To: <Undisclosed.Recipients@dec1.peq.coppe.ufrj.br>
 From: F17753@earthlink.net
 Subject: we will do all the work for you                          8068
 Date: Fri, 15 Jun 2001 17:47:29 -0400
 Mime-Version: 1.0
 Content-Type: text/html;
       charset="iso-8859-1"
 Content-Transfer-Encoding: quoted-printable
 X-Priority: 3
 X-Msmail-Priority: Normal
 Reply-To: kenlandel87@hotmail.com
 X-Spam-Suspect: SS
```

Muito embora na maioria dos casos se repita os endereços dos comandos SMTP **MAIL FROM** e **RCPT TO** respectivamente nos campos **From:** e **To:** das mensagens, isto não é obrigatório. Logo pela análise dos cabeçalhos de uma mensagem pode-se filtrar E-mails com um determinado campo **From:** que se repita em muitos SPAMs. Também pode-se filtrar campos **To:** que não contenham o endereço real do destinatário de uma mensagem (técnica muito usado pelos SPAMMERS) e pode-se filtrar ainda, no campo **Subject:**, um determinado assunto que seja repetido em muitos E-mails.

Outro tipo de filtragem feito pela análise dos cabeçalhos é através dos campos **Received:** de uma mensagem, onde pode-se filtrar mensagens que tenham se originado ou passado por um determinado servidor que esteja enviando SPAM (o que atualmente é impossível de ser feito em tempo real pelos servidores SMTP).

Existe ainda o campo **Date**, que indica a data e hora do remetente. É pratica bastante corrente dos SPAMMERS colocarem informações de data e hora no campo Date totalmente fora do especificado na RFC-2822 como, por exemplo, **Date: Domingo, 15 de Maio 2005, 01:00 Horário oficial da América do Sul**, quando o correto seria **Date: Sun, 15 May 2005 01:00:00 -0300**. Muitos SPAMMERS também costumam colocar o campo date com uma data e/ou hora futura porque muitos clientes de E-mails colocam os E-mail com data e/ou mais recente no inicio da listagem da caixa de entrada.

Como se pode ver, muitos SPAMs podem ser descartados por um aplicativo que faça uma simples analise de cabeçalhos de mensagem, desde que corretamente configurado.

5.3.2. A análise do conteúdo das mensagens

A filtragem de conteúdos de mensagens é **uma das técnicas ANTISPAM mais usadas a nível de usuário**. A lógica desta técnica é que, geralmente, as mensagens SPAMs costumam repetir com muita freqüência as mesmas expressões, frases ou períodos.

Um bom exemplo disso é o texto sobre o “105º Congresso Internacional de Bases Normativas sobre SPAM” ou ainda o texto “Esta mensagem não pode ser considerada SPAM se contiver um meio do destinatário ser removido da lista”. Se usarmos alguns aplicativos simples, como o filter do Unix, podemos jogar na lixeira todas as mensagens que vierem com estes textos. Geralmente, como os textos sofrem pequenas variações,

inclusive na língua em que são escritos, convêm ter as várias versões deles e colocar-se apenas fragmentos e não o texto completo para filtar.

Muitos usuários costumam configurar alguns softwares de análise de texto de mensagens, como o filter do Unix, para filtrarem mensagens que contenham um certo conjunto de palavras.

Por exemplo: sexo+pedofilia+grátis+aqui
new+offers+great+oppotunity

Pode-se ainda filtrar conteúdos de mensagens pelos campos CONTENT-<*> delas. Onde o <*> representa os diversos tipos de conteúdos que podem compor a mensagem, como HTML, TYPE (que engloba arquivos executáveis, arquivos DOC, PDF, etc). Desta forma pode-se inclusive descartar aquelas mensagens fraudadas do SPC, SERASA, etc e com um executável anexado apenas procurando-se pela existência do campo CONTENT-TYPE e examinando o seu conteúdo. Um exemplo:

```
Content-Type: APPLICATION/octet-stream; name="teste.exe"
Content-Transfer-Encoding: BASE64
Content-ID: <Pine.BSF.4.32.0103131604550.21582@gaia.coppe.ufrj.br>
Content-Description: Teste
Content-Disposition: attachment; filename="teste.exe"
```

Com exceção da filtragem pelos campos CONTENT-<*>, a técnica da filtragem por conteúdo tem a **deficiência de não conseguir filtrar mensagens de texto escrita dentro de imagens gráficas**, pois atualmente não existem softwares capazes de ler um texto escrito dentro de uma imagem gráfica. Dada a quantidade gigantesca de formatos gráficos existente atualmente (jpeg, gif, tiff, png, etc), é muito complexo se desenvolver um programa para esse fim e não será tão cedo que um surgira. Logo essa técnica é vulnerável ao **SPAM COM IMAGENS**.

Uma solução seria filtrar todos os campos CONTENT-TYPE apontando para imagens, porém ainda assim haveriam problemas com os E-mails não-SPAMs. Alem disso, teria que se filtrar E-mails com tags HTML apontando para imagens em sites remotos, o que seria inviável atualmente, uma vez que uma grande parte dos E-mails são escritos atualmente utilizando-se HTML.

5.3.3. A técnica da confirmação da autenticidade do remetente

Esta é uma **técnica oferecida por alguns ISP**, como **AntispamUOL** do Universo OnLine (UOL) [42], **e por alguns aplicativos**, como o **SafestMail** [43]. Ela tem pequenas variações, mas o principio de todas elas é que um remetente desconhecido pelo destinatário deve se identificar junto a este antes que a mensagem possa ser liberada para leitura.

Esta **técnica serve para barrar os E-mails enviados por robots** (softwares) SPAMMERS automáticos, pois estes não possuem a lógica humana para agir quando uma mensagem pede para eles se identificarem (quando existem E-mail de retorno valido para o SPAM enviado).

No engenho do **AntispamUOL**, quando um E-mail é recebido e o usuário do UOL não tem o endereço do remetente na sua relação de liberados, um E-mail é enviado pelo sistema para o endereço do remetente (obtido no campo To:) informando que o mesmo deve entrar no link informado no corpo do E-mail para liberar a mensagem.

Tal link leva a uma página onde uma **imagem com um texto** (caracteres alfanuméricos) é gerada em tempo real e a pessoa deve escrever o texto que lê na imagem. **Como já foi dito, nenhum software atualmente consegue ler textos dentro de imagens, isto vale para os robots SPAMMERS também**.

Fig.2 - Exemplo de texto em imagem gerado por software

O software **SafestMail**, funciona de modo semelhante ao AntispamUOL, porém como não é um sistema corporativo para vários usuários, mas um aplicativo de usuário, este envia um E-mail automático (quando o usuário for usar o cliente de E-mail dele) em que o remetente deverá informar o assunto que ele quer tratar com o destinatário da mensagem. Por **assunto** estenda-se **uma strings de tamanho limitado**, para evitar que uma string contendo um endereço com propaganda seja enviada.

Ambos, os sistemas e os softwares, são excelentes para o bloqueio de SPAMs originados dos robots SPAMMERS (ou spambots, como também são conhecidos). Porém existem alguns problemas relacionados ao funcionamento dessa técnica, alguns que necessitam da correta configuração dos sistemas ou softwares pelo usuário para evitá-los, outros que não haverão de como serem evitados. São eles:

- O usuário deve **colocar todos os remetentes autorizados**, e **todos os endereços de destinatários autorizados utilizados por ele**. Por exemplo, ele deve colocar todos os endereços das listas de discussão, que ele assine e que venham preenchido no campo To: do cabeçalho da mensagem, senão o sistema ou o software irá disparar E-mails automáticos para as listas de discussão, o que irritará muitos usuários de tais listas.
- Ainda sobre o que foi falado acima, **se a lista de discussão não tiver proteção contra SPAM**, quaisquer **SPAMs enviados para a lista serão recebidos pelo usuário**.
- **Se a lista de remetentes autorizados for descoberta o usuário ficará vulnerável**, porque o sistema ou software somente analisará o campo From da mensagem (será inviável o sistema ou software tentar analisar a origem do E-mail, pois poderá cair em muitos resultados “falso-positivos”.
- A proteção **pressupõem que se trata de um spambot** (software) que possui “inteligência” limitada, **mas muitos SPAMMERS contratam pessoas para a tarefa de burlarem esses casos “excepcionais”**, o que significa autorizar manualmente em sistemas como o AntispamUOL, ou tentar enganar habilmente o destinatário, como no caso do SafestMail.

- Está-se começando a desenvolver uma **nova geração de vírus, worms e Trojans** que, ao invadirem a máquina de um usuário, **irão exportar as listas de endereços (bookmarks) do mesmo para máquinas SPAMMERS**, e desta forma os usuários de tais sistemas ou softwares poderão passar a ficarem vulneráveis novamente a SPAMs originados de spambots que poderão mascarar-se como remetentes autorizados.

Pode-se dizer ainda que **embora tenham resultados bastante satisfatórios para os usuários finais, esses sistemas e softwares acarretam um aumento do trafego SMTP**, o que **prejudica mais a largura de banda do canal de comunicação externo das redes**, alem de **exigirem mais dos recursos dos sistemas**, pois os E-mails, independentes de serem SPAMs ou não, devem ser armazenados por um certo período de tempo, a espera do contato do remetente (normalmente e 3 a 5 dias, conforme a configuração do sistema ou do software).

Disto que foi discorrido acima, **surge mais uma vulnerabilidade grave**: Os sistemas ficam muito **vulneráveis a ataques de DDoS** (**Deny of Service**), pois vários SPAM-SPOOFING poderiam simplesmente acabar com o espaço em disco disponível, pressupondo que todos os endereços de remetentes estejam corretos. Nos ISP isso é prevenido prevendo-se de ante-mão sistemas com discos de altíssima capacidade. Nos computadores pessoais dos usuários, a alternativa é trabalhar com períodos de armazenamento menores ou discos de capacidades maiores, mas nunca rodar tais softwares com pouco espaço em disco.

Ainda que tais problemas talvez tenham uma **possibilidade remota de acontecer**, se deve ter em mente que eles **podem acontecer realmente**. Porém o usuário não deve ficar temeroso em usar sistemas ou softwares que implementem essa técnica apenas por causa de tais problemas.

5.3.4. A técnica da pontuação da mensagem

A técnica da pontuação da mensagem é utilizada por alguns plugins de MTA, como o Spam-Assassin (2ª linha de defesa), porém é mais utilizada por softwares finais de usuários (3ª linha de defesa), por isto está aqui descrita.

A técnica da pontuação da mensagem é inspirada na técnica da analise do conteúdo da mensagem, porém com uma pequena nuance que difere uma da outra:

- A **técnica da analise do conteúdo** procura por palavras especificas ou conjunto de palavras.
- A **técnica da pontuação** atribui valores para cada palavra encontrada e lhe atribui um valor, palavras relacionada a SPAMs recebem valores elevados. No final, os valores são somados e, a partir de um patamar atingido ou ultrapassado, a mensagem pode ser descartada ou marcada como SPAM no subject, como faz o Spam-Assassin.

Para um exemplo simples da técnica da pontuação, vamos imaginar uma mensagem contendo apenas a frase **“Acesse e veja as garotas fazendo sexo anal”**, vamos dizer que o patamar seja 100 e atribuímos os valores **40 para a palavra sexo**, **30**

para a palavra garotas, **40 para a palavra anal** e **0 para as demais palavras**. O software totalizaria 110 e adicionaria ao titulo (subject) da mensagem um aviso como "[SPAM Suspected]".

É claro que este é um exemplo muito simplificador, mas descreve bem a metodologia desta técnica.

A fraqueza desta técnica é que ela é vulnerável ao **SPAM COM IMAGENS**, uma vez que, como já foi visto, não existe nenhum software atualmente que leia textos escritos dentro de imagens gráficas.

5.3.5. Cuidados especiais para evitar de entrar em listas de SPAMMERS

O velho ditado já dizia: "**Melhor prevenir do que remediar**". A seguir algumas dicas úteis para evitar de entrar em listas de SPAMMERS:

- **NUNCA** divulgue teu E-mail abertamente em paginas HTML na Internet, pois fatalmente os robots **WEB-SPAM** irão catalogá-lo.
- Se tiver que colocar teu E-mail em páginas HTML na Internet, procure **usar scripts** (Javascript, Java, etc) que irão **gerá-los dinamicamente** num browser com suporte a Javascript, Java, etc. Uma alternativa é colocar o teu E-mail em uma imagem gráfica, tipo jpeg ou gif, assim somente um ser humano poderá lê-lo. **No código HTML do resumo** (página de abertura inicial da versão HTML deste trabalho) **há um Javascript que gera dinamicamente os dois E-mails lá mostrados**.
- Crie páginas que **geram links e E-mails falsos antes do teu E-mail**. Isso ira enganar e diminuir a performace dos **WEB-SPAM**. O uso de alguns scripts CGI em perl são muito bons para criar E-mails falsos e os disponibilizar. Por exemplo, o WPoison [14].
- Se receber um SPAM, **nunca o responda nem clique em link nenhum** que informe que clicando ali o teu E-mail será removido. Provavelmente você estará confirmando a validade do teu E-mail para o SPAMMER.
- Use **softwares ANTISPAM** e peça que o administrador da tua rede que configure o servidor SMTP dela com configurações ANTISPAM e plugins antivírus.
- Rode sempre um **antivírus atualizado na tua máquina**, isto ajudará a evitar worms ou trojans que enviem as tuas listas de endereços (bookmarks) para os SPAMMERS.
- **Apenas repasse os teus E-mails pessoais para pessoas confiáveis**.
- **Tenha sempre mais de um E-mail**. Um para as coisas sérias, outro para as coisas pessoais e outro para o resto. Se tiver que divulgar, divulgue o último.
- **Cuidado quando preencher formulários** que, entre os campos obrigatórios, exigem um E-mail de contato.
- **Cuidado quando acessar páginas na Internet**, principalmente as estranhas que você nunca tenha acessado. Utilize um browser (navegador) seguro para isso.

6. Conclusões Finais

Vimos neste trabalho que a prática do SPAM teve origens na “fragilidade” ou melhor dizendo “flexibilidade” com que o protocolo SMTP foi desenvolvido, potencializado pela entrada do comércio eletrônico na Internet.

O SPAM não começou da noite para o dia, como foi visto, ele foi um processo que começou devagar inicialmente e a partir de um certo momento, diríamos na segunda metade de 1997, teve uma expansão rápida após isso.

A pratica do SPAM não é realizada apenas por pessoas que desconheçam as etiquetas da Internet e achem que tudo nela é livre. Vemos que existem SPAMMERS altamente profissionais em enviar mensagens não-solicitadas e tentar fazê-las chegar aos nossos endereços eletrônicos com o maior sucesso possível.

O SPAM gera um custo muito grande para as redes ligadas na Internet, que se traduz em termos de gastos com a largura de banda do canal de comunicação externo da rede, gastos nos tempos de processamento das CPU, gastos em espaço de disco ocupado e gastos em termos de homem/hora para ler e apagar SPAMs recebidos.

A pratica não é ainda objeto de uma ação mais forte do governo brasileiro, como o deveria ser. Com isso, as redes do Brasil acabam sendo mal-vistas nos outros paises, como possíveis fontes de SPAMs.

As técnicas ANTISPAM foram sendo desenvolvidas em paralelo com o crescimento das técnicas SPAMs. Porém essa é uma guerra que não terá fim tão cedo, pois para a ação de um lado existe sempre uma resposta do outro.

As técnicas ANTISPAM desenvolvem-se em três linhas de defesa: A 1ª linha que são as técnicas implementadas para os servidores SMTP (MTA), que visam proteger a largura de banda do canal de comunicação externo das redes, os recursos dos sistemas ligados nas redes e os usuários finais das redes. A 2ª linha de defesa visa proteger os recursos dos sistemas, os gastos em termos homem/hora para ler e apagar SPAMs (ou seja, os usuários finais das redes). A 3ª linha de defesa visa ser a última proteção possível para os próprios usuários finais.

Cada técnica ANTISPAM tem seus pontos positivos e negativos e cabe aos administradores de redes e/ou os usuários delas definirem um bom termo para as utilizarem.

7. Bibliografia

1. Lutus, P.; The Anti-Spam Home Page, http://www.arachnoid.com/lutusp/antispam.html, U.S.A., 1999.
2. Mail Abuse Prevention System LLC (MAPS), http://mail-abuse.org, U.S.A., 1997-2005.
3. Network ABUSE Clearinghouse, http://www.abuse.net, U.S.A. 2004.
4. The SpamHaus Project, http://www.spamhaus.org, U.K. 2000-2005.
5. Fight Spam on the Internet, http://spam.abuse.net, U.S.A. 1996-2005.
6. Spam Pesters Admins about Mail-abuse, http://spam.sourceforge.net, U.S.A. 2000-2001.
7. SpamCop.net, http://spamcop.net, U.S.A., 1998-2005.
8. Coalition Against Unsolicited Commercial Email, http://www.cauce.org, U.S.A., 1997-2005.
9. Movimento Brasileiro do Combate ao Spam, http://www.antispam.org.br, Brasil, 1998-2005.
10. Sendmail Consortium, Sendmail Project, http://www.sendmail.org, U.S.A., 1990-2005.
11. Venema's, Wietse, The PostFix Home-Page, http://www.postfix.org, U.S.A., 2000-2005.
12. Bernstein, Dan, The qmail Home-Page, http://www.qmail.org, U.S.A., 1996-2005.
13. University of Cambridge, The Exim Home-Page, http://www.exim.org, U.S.A., 1996-2005.
14. E-Scrub Tecnologies Inc, WPoison, http://www.monkeys.com/wpoison, U.S.A., 1997-2000.
15. Szendrodi, Rafael J. C., Antispam-UFRJ, http://www.aupads.org, Brasil, 2002-2005.
16. Grupo Brasil Antispam,. http://brasilantispam.org, Brasil, 2005.
17. Harris, Evan; GreyListing – The Next Step in Spam Control War, http://projects.puremagic.com/greylisting, U.S.A., 2003.
18. B. Postel, Jonathan and Sluizer, Suzanne; Mail Transfer Protocol (RFC-772), http://www.ietf.org/rfc/rfc0772.txt?number=772, U.S.A., 1980.
19. B. Postel, Jonathan and Sluizer, Suzanne; Mail Transfer Protocol (RFC-780), http://www.ietf.org/rfc/rfc0780.txt?number=780, U.S.A., 1981.
20. B. Postel, Jonathan; Simple Mail Transfer Protocol (RFC-788), http://www.ietf.org/rfc/rfc0788.txt?number=788, U.S.A., 1981.
21. B. Postel, Jonathan; Simple Mail Transfer Protocol (RFC-821), http://www.ietf.org/rfc/rfc0821.txt?number=821, U.S.A., 1981.
22. Klensin, J.; Simple Mail Transfer Protocol (RFC-2821), http://www.ietf.org/rfc/rfc2821.txt?number=2821, U.S.A., 2001.
23. B. Postel, Jonathan; Internet Message Protocol (RFC-753), http://www.ietf.org/rfc/rfc0753.txt?number=753, U.S.A., 1979.
24. Crocker, David H.; Standard for the format of ARPA Internet Text Messages, http://www.ietf.org/rfc/rfc0822.txt?number=822, U.S.A., 1982.

25. Resnick, P.; Internet Message Format, http://www.ietf.org/rfc/rfc2822.txt?number=2822, U.S.A., 2001.
26. Domain Names – Concepts and Facilities, http://www.ietf.org/rfc/rfc1034.txt?number=1034, U.S.A., 1987.
27. Domain Names – Implementation and Specifications, http://www.ietf.org/rfc/rfc1035.txt?number=1035. U.S.A., 1987.
28. Barr, D.; Common DNS Operational and Configuration Errors, http://www.ietf.org/rfc/rfc1912.txt?number=1912, U.S.A., 1996.
29. Internet Engineering Task Force; MARID – MTA Authorization Records in DNS, http://www.ietf.org/html.charters/OLD/marid-charter.html, U.S.A., 2004.
30. MARID to close, http://www.imc.org/ietf-mxcomp/mail-archive/msg05054.html, U.S.A., 2004.
31. Levine, John; An Analysis of Microsoft's MARID Patent Applications, http://www.circleid.com/article/756_0_1_0_C, U.S.A., 2004.
32. The UUCP Project, http://www.uucp.org, U.S.A., 2000.
33. ABC news, http://abcnews.go.com/Technology/wireStory?id=653257, U.S.A., 2005.
34. Jornal Eletrônico Novo Milênio; Nosso e-glossário, http://www.novomilenio.inf.br/glossar/eglosss.htm, Brasil, 2001.
35. Wikipedia, The Free Encyclopedia; The SPAM (Monty Python) http://en.wikipedia.org/wiki/Spam_(Monty_Python), U.S.A., 2005.
36. Computer Dictionary,Webopedia; SPAM, http://www.webopedia.com/TERM/s/spam.html, U.S.A., 2004.
37. Spam-Site.com; What is spam?, http://www.spam-site.com/what_is_spam.shtml, U.S.A., 2005.
38. Folha Online Informática, Brasil é o 4o maior remetente de spam do mundo, diz ONU, http://www1.folha.uol.com.br/folha/informatica/ult124u14532.shtml, Brasil, 2003.
39. Newsreader – Newsgroups online, Reject Mails from IP's without reverse DNS, http://www.issociate.de/board/post/195936/Reject_mail_from_IP's_without_reverse_DNS.html, Alemanha, 2004.
40. Rickert, Neil; Neil Rickert's configuration hacks, http://www.cs.niu.edu/~rickert/cf, U.S.A., 2003.
41. Apache Software Foundation, The Apache SpamAssassin Project, http://spamassassin.apache.org, U.S.A., 2005.
42. Universo OnLine, Antispam UOL, http://email.uol.com.br/antispam, Brasil, 2005.
43. SafestMail, SafestMail, http://www.safestmail.com.br, Brasil, 2005.
44. CBEJI – Centro Brasileiro de Estudos Jurídicos da Internet, Sentenciado primeiro caso de spam no Brasil , http://www.cbeji.com.br/noticias/noticias1612-1601.htm#Sentenciado%20o%20primeiro%20caso%20de%20spam%20no%20Brasil, Brasil, 2002.
45. CBJI - Centro Brasileiro de Estudos Jurídicos da Internet, Spam liberado – *Mensagem indesejada não corresponde a pratica abusiva* , http://www.cbeji.com.br/noticias/noticias1612-1601.htm#Spam%20liberado%20-%20Mensagem%20indesejada%20n%E3o%20corresponde%20a%20pr%E1tica%20abusiva, Brasil, 2001.