SPAM: Levantando uma discussão

Por: Fernando Verissimo
Novembro/2003

Todos nós estamos recebendo muitas mensagens de correio eletrônico indesejadas. Isso vem nos irritando muito. Nos irrita por vários motivos: Enche nossa caixa postal; deixa a rede mais lenta; nos faz perder mensagens importantes na nossa pressa de debilitar o lixo; e principalmente, nos faz perder tempo.

No jargão da computação, essas mensagens indesejáveis têm um nome: SPAM. O nome SPAM (SPiced hAM) vem de uma marca de presunto dos EEUU, fabricada nos anos 30. O portal Terra[1] conta que em um quadro de um programa do grupo Monty Python na TV inglesa na década de 70, eles encenaram uma cena surreal em um restaurante que servia todos os seus pratos com SPAM. A garçonete descreve para um casal de clientes os pratos repetindo a palavra "spam" para sinalizar a quantidade de presunto que é servida em cada prato. Enquanto ela repete "spam" várias vezes, um grupo de vikings que está em outra mesa começa a cantar "Spam, spam, spam, spam, spam, spam, spam, spam, lovely spam! Wonderful spam!", interrompendo-a.

Por isso, alguns usuários dos MUDs (multi-user dungeon, um antigo ambiente compartilhado usado para bate-papo virtual) começaram a fazer o paralelo entre a irritante e repetitiva música "spam" e as mensagens repetitivas e irritantes de alguns usuários que anunciavam produtos ou idéias. Existem também relatos de usuários usando scripts que digitavam "...spam, spam..." automaticamente nas salas de bate-papo, em 1985. Em pouco tempo, os usuários da Usenet, maior sistema de grupos de notícias e listas de discussão online, adotaram o termo. O primeiro spam via e-mail documentado foi enviado em 3 de maio de 1978, há 25 anos. Já o uso do termo spam na Usenet completou 10 anos em março de 2003.

Há pesquisas que dizem que, no mundo, mais da metade dos correios eletrônicos que circulam são spams. Isso se torna mais assustador se soubermos que em 2000 o percentual de mensagens indesejadas na rede era de 8%. Como estaremos em 2005? Aqui na ABC, eu não preciso de pesquisas para dizer que temos bem mais do que média mundial. O extremo é o endereço coorporativo da ABC, abc@abc.org.br, que nas 24 últimas horas recebeu 378 mensagens: 3 de Joanna Lacey, 2 de Yves Quere, ambos ligados à IAP, e as demais mensagens eram SPAMs. Absurdo, não? Isso, quer dizer, se por um descuido eu não apaguei mensagens que não eram SPAMs. Vocês são capazes de imaginar quanto tempo eu levo diariamente para abrir essas 300 mensagens. Mais do que gostaríamos.

Mais preocupante é o crescimento do número de vírus, vermes, backdoors, e outros softwares maliciosos que se aproveitam desses SPAMs para se distribuir. O outro problema é o crescimento do número de fraudes. Essa

[1] http://www.terra.com.br

semana eu li no Jornal O Globo que o Banco Central alertava para as mensagens falsas que se diziam oriundas da rede bancária, pedindo ao usuário ou cliente o recadastramento de seus dados. O cliente deveria acessar o tal link que era lhe informado e passar número de conta e senha para o bandido.

Eu recebo mensagens de todo tipo, algumas que querem me vender parafusos em Pindamonhangaba (é assim que escreve?), é só passar lá, aparelhos que prometem aumentar o órgão sexual masculino, vários que só contém caracteres aleatórios sem nenhuma informação. É um absurdo!

Vejam que eu não estou falando de mensagens que querem a presença do presidente da ABC numa feira de ciência de uma escolinha qualquer, pois até essas têm alguma finalidade.

Não há solução fácil para esse problema, por enquanto. Alheios ao tormento que causam, os spammers, como são chamados os que espalham SPAMs, rechaçam as tentativas de controle, tomando emprestado a bandeira de liberdade de expressão, e dão um jeito de invadir a nossa caixa postal. E é fácil fazer isso, basta comprar um CD com uma base de dados contendo os nossos endereços, que vêm junto um software que ajuda a distribuir os SPAMs.

Distribuição

São três as técnicas de distribuição: Entrega direta; open relay e open proxy.

Os programas de entrega direta monta um servidor SMTP no computador do spammer, localizam os servidores de correio eletrônico de um determinado provedor de acesso e disparam os emails por vários ao mesmo tempo. Esses são mais fácil de serem rastreados.

A segunda técnica mais comum faz uso de um programa que varre a Internet a procura um conjunto de servidores open relay, aqueles que estão com o serviço de email mal configurado, permitindo o acesso a qualquer um que se conecte a eles. Quando encontram, conectam-se e disparam mensagens. Há tempos nós somos obrigados a passar login e senha para acessar o servidor SMTP da ABC.

Há um terceiro método em que o programa de distribuição de SPAMs varre a Internet a procura de proxies abertos. Proxy é um servidor que acessa a informação na Internet na primeira vez que ela é requisitada e passa a fornece-la imediatamente à medida que novas requisições são feitas a ela. Serve para agilizar a busca à Internet. A ABC tem um proxy integrado ao seu firewall. Como todo pacote enviado à Internet por uma rede é feito pelo seu proxy, ele (pacote) é assinado pelo IP do proxy. O spammer se aproveita dos proxies que estão abertos para esconder o seu próprio endereço IP e assim não poder ser rastreado. Proxies abertos não falta na internet, no dia 18 de setembro de 2003, o site Blitzed.org registrava média de 29.045 proxies abertos.

Resolvido o problema de como enviar, basta garantir que o email vá chegar ao destino, ou seja, até nós. A maneira mais fácil é comprar um CD que contenha uma base de dados de endereços. Essas bases são montadas por pessoas que passam o seu tempo procurando emails enviados para várias

pessoas que ficam registrados na internet ou em listas de discussões e elas vão copiando cada endereço e montando uma base. Outra maneira é montar uma base de dados dos domínios (abc.org.br; uol.com.br; hotmail.com) e usar os logins mais comuns, que existem em qualquer domínio. Desta forma, carlos@abc.org.br tenderia a receber mais SPAMs do que cerm@abc.org.br ou crs@abc.org.br; sandra@abc.org.br mais do que sfcarvalho@abc.org.br. E pela razão anterior, verissimo@abc.org.br, o usuário mais antigo do nosso domínio, tenderia a receber mais SPAMs do que amelia@abc.org.br, com o login criado há pouco tempo.

O spammer também precisa que a vítima abra a mensagem e para isso usa algumas artimanhas, como colocar alerta sobre novo vírus encontrado, alguma correção para falhas de segurança no Windows, alerta sobre as novas medidas do MEC sobre o portal periódicos, etc....

Contra-ataque

O spammer tem que ser chato, pois é notório que o retorno de mala direta é de 1%, quando a mala direta é pela internet esse número cai ainda mais.

A listra negra é uma solução ineficaz. Nas listas negras nós cadastramos os endereços dos spammers, e os filtros de mensagens podem usar essas listas para filtrar mensagens oriundas dos spammers. Existe mais de 200 listas negras na internet, mas graças ao open relay, o spammer se utiliza de endereços inválidos, até de válidos que pertencem a não spammers. Isso quer dizer que um spammer pode se utilizar de um stmp open relay e enviar uma SPAM como se tivesse sido enviado por storino@abc.org.br, por exemplo[2].

Existem também os programas de filtragens. Eles funcionam de três formas: a primeira, como eu já citei, é se utilizando das listas negras. A segunda seria se utilizando das listas brancas. O usuário teria uma lista branca com os endereço de seus correspondentes, e toda mensagem que não estivesse castrada em sua lista branca seria filtrada.

A lista branca é o método, ou um dos métodos adotados pelo provedor de acesso UOL (universo online). Vocês já devem tem observado que algumas das mensagens enviadas para o um cliente do UOL retornam com um pedido estranho, pedem para você acessar um link na internet que contém uma imagem com umas letras, e pedem para você escrever as letras num campo determinado. Se o que você escreveu confere com a imagem mostrada, a mensagem que você enviou segue para o destino. Isso é porque ainda não inventaram um software de distribuição de SPAMs que leiam tais imagens e transcrevam as letras. O processo até agora só pode ser feito por um humano. E acredita-se que o spammer que envia 100.000 mensagens de uma vez só, através de um software de distribuição, não perderá tempo com isso. As letras

[2] Esse episódio aconteceu realmente. O Dr. Francisco Storino veio a minha sala assustado com o fato de pessoas, aqui dentro da ABC, terem recebido SPAMs vindo dele, sem ele ter feito tal operação.

são mostradas em fontes[3], cores, formatos, posição e orientação[4] distintas, dificultado a vida de um software reconhecedor de imagens.

O terceiro método é o de classificação do SPAM por estatística de palavras-chaves. Esses filtros fazem uma análise da mensagem, procurando palavras previamente cadastradas, tais como Viagra, pênis, sexo, e dando valores a elas. A soma das características vai dar uma pontuação que definirá a mensagem como spam ou não.

Podemos ainda combinar os três métodos. Os três métodos trazem problemas. A lista negra é discriminatória, pode acarretar processos jurídicos contra as entidade que as mantém. A lista branca inibe novos contatos. Eu, particularmente, parei de enviar mensagem para o UOL. E o método estatístico pode provocar a filtragem de uma mensagem que não deveria ser filtrada. Um exemplo: A nova música cantada pela Rita Lee com letra do Arnaldo Jabor, "Amor e Sexo", tem a palavra sexo em cada frase. A pontuação de uma mensagem que contivesse a letra daquela música seria muito alta, com certeza seria descartada. Só que essa letra poderia estar sendo enviada entre dois amigos, fãs de Rita Lee, que certamente não gostariam de ter suas mensagens filtradas.

O valor máximo de pontos que uma mensagem a ser aprovada pelo filtro estatístico poderia ter, e o valor de cada palavra requereria ajustes: SPAMs aprovados (falso negativos) e mensagens "boas" reprovadas (falso positivo) aconteceriam com muita freqüência no início dos ajustes. Uma rede que quisesse implantar esse método passaria por dificuldades no início da implantação.

Eu gostaria de implantar o método estatístico. Será que a Academia estaria disposta a passar pelos ajustes?

Comportamento adequado

Até a solução definitiva e em paralelo, existem algumas posturas e alguns comportamentos que podemos ter para diminuir os SPAMs. Segue alguns exemplos[5]:

1. Peça para a Informática mudar o seu login: bianca@abc.org.br; bianca@uol.com.br; bianca@mct.gov.br; bianca@globo.com; são exemplos de email que estão cadastrados em qualquer base de dados de spammers. A probabilidade de haver uma Bianca num domínio de internet é muito grande. Lembro que há algum tempo conseguir promover a mudança de email do Humberto, da Márcia, do Carlos e da Sônia. Pergunte a eles, o que tiveram que fazer para se re-adequar ao novo email.
2. Cultive várias contas: uma profissional, uma pessoal para coisas sérias e outra para distribuir para estranhos.

[3] Uma em Times New Roman, outra em Arial, outra em Courier, etc...
[4] Na vertical ou em orientação inclinada.
[5] Alguns itens foi escrito por mim, mas a maioria foi tirada da revista InfoExame de Outubro/2003

3. Evite divulgar seu email em chats, sites, blogs e grupos de discussão. Quando for inevitável, use a terceira conta.
4. Não responda ao SPAM. A sua resposta é uma confirmação de sucesso e o encorajamento que mais SPAMs sejam enviados.
5. Engane os softwares de busca de endereços de correio eletrônico. Ao escrever o seu endereço na web, troque os sinais de @ e ., pelas palavras arroba e ponto ou at e dot. Ex.: verissimoATabcDOTorgDOTbr.
6. Ao enviar mensagens com cópia, use a oculta, para não expor os destinatários aos caçadores de endereços, e recomende essa opção a seus contatos mais freqüentes.
7. Em páginas web que perguntam se você quer receber informações de parceiros comerciais,marque apenas as muito interessantes.
8. Não preencha formulários em sites que não tiverem uma política de privacidade severa.
9. Em conexão de banda larga, evite que spammers use seus recursos, bloqueando o acesso externo com um firewall e desligando o servidor de SMTP do compatilhador de arquivos se usa um.
10. Desconfie sempre de emails enviados por empresas que pedem suas informações pessoais. Na dúvida, delete a mensagem.
11. Nunca clique em arquivos suspeitos que acompanha a mensagem.

Fernando Verissimo é Analista de Sistemas, gerente de Informática e Tecnologias da Academia Brasileira de Ciências, aluno do mestrado em Redes de Computadores do Programa de Engenharia de Sistemas e Computação da COPPE/UFRJ.