

SPAM

Alexandre Marin Tuxen, Jean Cleber Correia, José Mario Souza, Thiago Bueno Nahum

Resumo — Em plena era de Internet comercial, o spam é uma das principais perturbações para internautas, administradores de redes e provedores, de tal forma que o abuso desta prática já se tornou um problema de segurança de sistemas. Além disso, é também um problema financeiro, pois vem trazendo perdas econômicas para uma boa parte dos internautas e lucro para um pequeno e obscuro grupo. Além de fazer uso indevido de informações cadastrais dos usuários, as mensagens SPAM têm como objetivo sobrecarregar a capacidade dos servidores, já que são enviadas em massa, comprometendo a qualidade dos serviços, as redes de comunicação e a própria caixa de mensagens do usuário, com parte de seu espaço em disco consumido pelas mensagens SPAM.

Palavras Chave — spam, internet, e-mail, smtp

I. INTRODUÇÃO

O termo Spam, abreviação em inglês de “spiced ham” (presunto condimentado), é uma mensagem eletrônica não-solicitada enviada em massa. O spam também é conhecido pela sigla inglesa UCE (Unsolicited Commercial Email, ou Mensagem Comercial Não-Solicitada). Na sua forma mais popular, um spam consiste numa mensagem de correio eletrônico com fins publicitários.

O termo spam, no entanto, pode ser aplicado a mensagens enviadas por outros meios e noutras situações até modestas. Geralmente os spams têm caráter apelativo e na grande maioria das vezes são incômodos e inconvenientes. Atualmente, devido à facilidade de disseminação de spam e também devido à própria concepção do protocolo SMTP que, na época de seu desenvolvimento, não tinha o foco na segurança e sim na funcionalidade fez com que o spam se tornasse um dos principais problema a ser resolvido. O objetivo do artigo é entender como funciona e as técnicas de distribuição em massa de e-mails e também entender as principais técnicas tecnológicas hoje existentes para diminuir esse tipo de mensagens.

II. PREJUÍZOS CAUSADOS

Simultaneamente ao desenvolvimento e popularização da Internet, ocorreu o crescimento de um fenômeno que, desde seu surgimento, se tornou um dos principais problemas da comunicação eletrônica em geral: o envio em massa de mensagens não-solicitadas. Esse fenômeno ficou conhecido como spamming, as mensagens em si como spam e seus autores como spammers.

Apesar da existência de mensagens não-eletrônicas que podem ser comparadas a spam, como por exemplo

folhetos promocionais não-solicitados, o termo é reservado aos meios eletrônicos devido a motivações que tornam tais meios muito mais propícios ao crescimento do fenômeno do que outros.

Embora algumas leis a respeito do assunto já tenham sido aprovadas, ainda não existe uma legislação definitiva que regule a prática do spamming ou a caracterize como sendo crime. Apesar desta atual indefinição legal, diversas entidades governamentais, comerciais e independentes declaram que o spam é um dos maiores problemas atuais da comunicação eletrônica.

No Brasil não é crime enviar spam, mas esta prática acaba sendo autoregulamentada, pois o spammer é mal visto, seu produto ou empresa é desacreditado, seu provedor, domínio ou IP pode ser incluído nas listas de bloqueio dos administradores de rede. Por este motivo quase sempre o spam está ligado a práticas criminosas ou a ingenuidade do empreendedor.

Os raros casos de prisão ou citação de spammers são provenientes do crime cometido por eles e não do envio do spam em si. Exemplos: enviar spam se fazendo passar por outra pessoa ou empresa, enviar spam com programas maliciosos, destinados a invadir sistemas ou capturar senhas. Nestes casos a prisão se deu pelo crime cometido e não pelo spam (que ainda não é considerado crime). Os softwares de filtro de spam por mais preciso que sejam, acabam bloqueando e-mails válidos, muita das vezes importantes e que podem até gerar prejuízo para a empresa.

Além do problema do não recebimento de e-mails importantes há um gasto desnecessário de tempo por parte do usuário que recebe o spam e acaba tendo que ler, identificar e remover o e-mail da sua caixa postal, uma média de 16 segundos por mensagem de spam, sendo assim caindo a sua produtividade uma vez que o usuário necessita do e-mail para desenvolver seu trabalho.

Tais mensagens também pode vir acompanhada de um conteúdo impróprio ou ofensivo devido ao grande numero de pessoas que são enviadas, ou podem vir de links de sites que tentam fraudar instituições financeiras, instituições do governo ou até mesmo programas maliciosos programados para coletar os dados pessoais e financeiros.

Em uma pesquisa desenvolvida pela Nucleus Research e divulgada pela Computerword mostra que apesar dos filtros de spam, 66% dos e-mails nas caixas postais são lixo eletrônico e que este lixo eletrônico chega a custar 712 dólares ou 1.330 reais por funcionário, por ano, para as empresas.

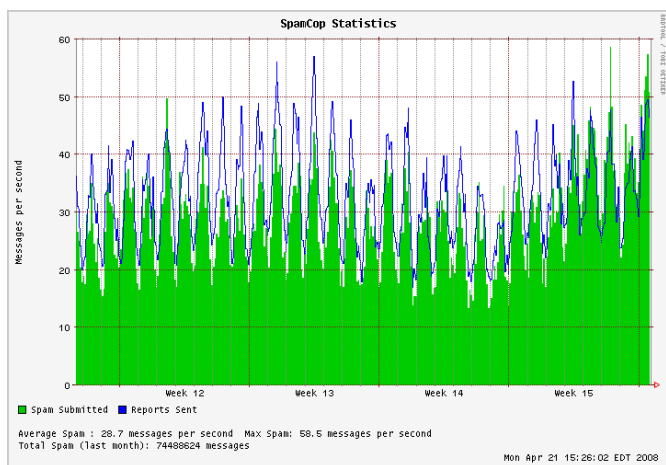


Fig. 1. quantidade de spam enviados no mês de abril [1]

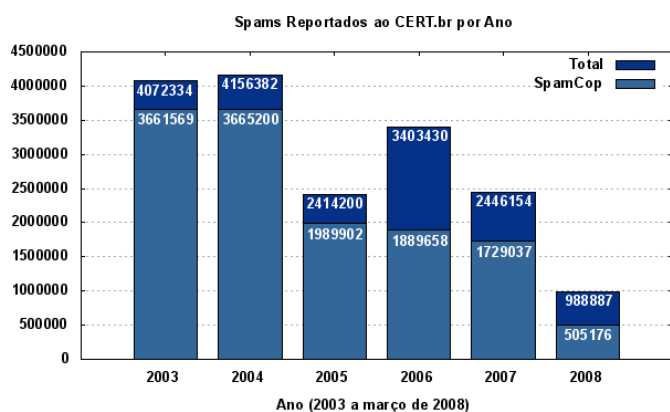


Fig. 2. Quantidade de spam enviados durante os últimos 5 anos [2]

III. TIPOS DE SPAM

- **Boatos (hoaxes)**

O termo hoax está associado a histórias falsas, escritas com o intuito de alarmar ou iludir aqueles que a lêem e instigar sua divulgação o mais rapidamente e para o maior número de pessoas possível. Geralmente tratam de pessoas que necessitam urgentemente de algum tipo de ajuda, alertas a algum tipo de ameaça ou perigo, difamação de marcas e empresas ou ofertas falsas de produtos gratuitos. Aquelas que relatam histórias cujos personagens, época ou localização são desconhecidos são histórias conhecidas como "lendas urbanas".

Um exemplo bem conhecido de boato enviado por spammers brasileiros menciona um livro de geografia usado em escolas norte-americanas que traz um mapa onde a Amazônia é considerada território internacional.

- **Correntes (chain letters)**

Mensagens desta categoria prometem sorte, riqueza ou algum outro tipo de benefício àqueles que a repassarem para um número mínimo de pessoas em um tempo pré-

determinado; garantindo, por outro lado, que aqueles que interromperem a corrente, deixando de divulgar a mensagem, sofrerão muitos infortúnios. Com esse mecanismo, elas têm a capacidade de atingir um número exponencial de pessoas em um curto período de tempo.

- **Propagandas**

Divulgam desde produtos e serviços até propaganda política. Este tipo de spam é um dos mais comuns e um dos mais antigos já registrados.

Embora existam mensagens comerciais legítimas, enviadas por empresas licenciadas e conhecidas, nota-se que não é raro que o produto ou serviço oferecido pela mensagem tenha alguma característica ilegal e o spammer e a empresa sejam desconhecidos do público ou completamente anônimos.

Entre outros, um spam publicitário costuma apresentar medicamentos sem prescrição, software pirata ou ilegal, diplomas universitários, oportunidades de enriquecimento rápido, cassinos e outros esquemas de apostas, produtos eróticos e páginas pornográficas. Um dos exemplos mais conhecidos do público é o spam que oferece o medicamento Viagra a baixo custo.

- **Golpes (scam)**

Tratam de oportunidades enganosas e ofertas de produtos que prometem falsos resultados. Entre as ofertas mais comuns estão as oportunidades miraculosas de negócios ou emprego, propostas para trabalhar em casa e empréstimos facilitados. Todos podem ser encontrados em uma lista elaborada pela Federal Trade Commission em 1998 que reúne 12 tipos comuns de fraudes e golpes relacionados a spam nos Estados Unidos na época.

- **Estelionato (phishing)**

São mensagens que assumem o disfarce de spam comercial ou cujos títulos simulam mensagens comuns, como comunicados transmitidos dentro de uma organização ou mensagens pessoais oriundas de pessoas conhecidas.

Tal disfarce tem como objetivo iludir o destinatário, solicitando-lhe que envie dados confidenciais (preenchendo um formulário, por exemplo) para algum endereço eletrônico ou que se cadastre em uma página da Internet que na verdade é uma cópia de alguma outra página. Na maioria dos casos, essas armadilhas são criadas para obter informações pessoais e senhas para que possam ser usadas em algum tipo de fraude ou para transferências bancárias e compras pela Internet.

- **Programas maliciosos**

De forma semelhante ao spam de estelionato, este tipo apresenta-se sob disfarce e induz o destinatário a executar um programa de computador malicioso enviado junto à mensagem. Dentre os programas usualmente enviados desta forma estão principalmente os vírus, os worms e os trojans.

- **Vírus**

Vírus são programas capazes de atingir arquivos e programas de um computador que tenha sido "infectado" através de sua execução. Como em cada um deles é inserido

uma nova cópia, esses arquivos ou programas passam a transmitir o vírus também. Embora existam vírus cuja única finalidade é perturbar o usuário do computador, a maioria deles age destrutivamente, corrompendo ou apagando arquivos e desconfigurando o sistema.

- **Worms**

Worms também são programas que se replicam e tentam atingir outros computadores, mas diferentemente dos vírus, não precisam de um arquivo para transportá-los. Um dos mais conhecidos foi o Sasser, cujo alvo eram computadores rodando os sistemas Windows XP e Windows 2000.

- **Cavalos de Tróia**

Os trojans, ou "cavalos de Tróia", são programas que desativam as medidas de segurança comuns de um computador em rede, permitindo que um programa sendo executado em outro computador adquira privilégios e possa, por exemplo, copiar, alterar e remover os arquivos e registros do computador em que o trojan está instalado. Existem cavalos de Tróia que inclusive forçam o computador atingido a repassar o spam para outros endereços.

- **Ofensivos**

Divulgam conteúdo agressivo e violento, como por exemplo acusações infundadas contra indivíduos específicos, defesa de ideologias extremistas, apologia à violência contra minorias, racismo, xenofobia e pedofilia.

IV. IMPACTOS DA PROPAGAÇÃO DO SPAM

Usuários

Os usuários do serviço de correio eletrônico podem ser afetados de diversas formas. Alguns exemplos são:

Não recebimento de e-mails: Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de spams recebidos seja muito grande o usuário corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, o usuário não conseguirá mais receber e-mails e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. O usuário também pode deixar de receber e-mails em casos onde estejam sendo utilizadas regras anti-spam ineficientes, por exemplo, classificando como spam mensagens legítimas.

Gasto desnecessário de tempo: Para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal.

Aumento de custos: Independentemente do tipo de acesso a Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado a Internet, cada spam representa alguns segundos a mais de ligação que ele estará pagando.

Perda de produtividade: Para quem utiliza o e-mail como uma ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de e-

mails, além de existir a chance de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

Conteúdo impróprio ou ofensivo: Como a maior parte dos spams são enviados para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

Prejuízos financeiros causados por fraude: O spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros. Este tipo de spam é conhecido como phishing/scam (maiores detalhes na Parte IV: Fraudes na Internet). O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas neste tipo de mensagem fraudulenta.

Provedores de acesso, backbones e empresas

Para as empresas e provedores os problemas são inúmeros e, muitas vezes, o custo adicional causado pelo spam é transferido para a conta a ser paga pelos usuários. Alguns dos problemas sentidos pelos provedores e empresas são:

Impacto na banda: Para as empresas e provedores o volume de tráfego gerado por causa de spams obriga a aumentar a capacidade de seus links de conexão com a Internet. Como o custo dos links é alto, isto diminui os lucros do provedor e muitas vezes pode refletir no aumento dos custos para o usuário.

Má utilização dos servidores: Os servidores de e-mail dedicam boa parte do seu tempo de processamento para tratar das mensagens não solicitadas. Além disso, o espaço em disco ocupado por mensagens não solicitadas enviadas para um grande número de usuários é considerável.

Inclusão em listas de bloqueio: O provedor que tenha usuários envolvidos em casos de spam pode ter sua rede incluída em listas de bloqueio. Esta inclusão pode prejudicar o recebimento de e-mails por parte de seus usuários e ocasionar a perda de clientes.

Investimento em pessoal e equipamentos; Para lidar com todos os problemas gerados pelo spam, os provedores necessitam contratar mais técnicos especializados, comprar equipamentos e acrescentar sistemas de filtragem de spam. Como consequência os custos do provedor aumentam.

V. TÉCNICAS USADA PARA ENVIAR SPAMS

Os spammers como são conhecidos os usuário que utilizam da forma de enviar e-mails em massa para disseminar mensagens sem solicitação, que tem como técnicas os mecanismos:

- **Programas de envio de e-mail em massa:** também conhecidos como programas de bulk mailing (mensagens em lote) ou mass mailing (mensagens em massa), onde sua função é enviar os e-mails para uma grande quantidade, onde eles podem ser configurados para enviar e-mails através de

máquinas com proxies abertos, onde estes proxies são máquinas mal configuradas ou estão instalados em máquinas contaminadas.

- **Spam zombies:** são computadores que foram infectados por códigos maliciosos, onde estes códigos permitem que o spammer utilize a máquina para o envio de spam.
- **Virus propagados por e-mail:** geralmente são recebidos por e-mail onde o mesmo procura induzir o usuário a clicar no arquivo anexado e ser infectado, ao ser infectado o cliente de e-mail envia cópias do e-mail infectado para a lista de contatos do usuário.
- **Abuso de formulários e scripts na web:** muitos serviços web tem algum tipo de transmissão de conteúdo de formulários por e-mail, sendo que tal funcionalidade pode ser abusada para a transmissão de spam. Um caso bem conhecido é o script CGI FormMail.pl, que envia o e-mail utilizando-se de informações providas no formulário e que pode ser abusado para prover anonimato para o spammer.
- **Uso de sites comprometidos:** alguns spammers utilizam servidores comprometidos para enviar spam, uma prática comum é a inclusão de alguma página web especial para o enviado de spam.
- **Spam baseado em imagem:** os spammers enviam mensagens de e-mail onde o anexo de imagens tenta confundir a ferramenta anti-spam variando levemente as imagens em cada mensagem, tornando difícil a detecção de spam único, uma vez que todas as assinaturas do spam são diferentes.

VI. TÉCNICAS ATUAIS PARA PROTECAO DE SPAMS

Para reduzir o volume recebido de spam e zelar pela própria segurança na Internet é fundamental um conjunto de medidas tecnológicas e de procedimentos de boas praticas.

Boas Praticas:

- Evitar se cadastrar em listas de discussão, sites e qualquer outro tipo de cadastro desconhecidos ou suspeitos
- Jamais clicar em links suspeitos

Tecnológicas:

- **DNS Reverso:** Técnica onde todo e-mail que chega é checado seu IP verificando-se se existe um domínio apontando para o mesmo.
- **Reverso MX:** Técnica onde todo e-mail que chega é checado se o domínio do remetente tem um servidor de MX
- **Black List:** Uma lista publica disponível na Internet onde é listado IPs considerados distribuidores de spams
- **Reconhecimento OCR:** Os spams cada vez mais enviam emails com figuras, o que dificulta o

bloqueio, mas existe técnicas de OCR que detectam as letras da imagem

- **Pontuação:** Um sistema que consiste em pontuações para varias partes do e-mail, ou seja, caso o e-mail atinja a pontuação configurada será considerado spam.
- **GrayListing:** Sistema onde a primeira conexão é bloqueada, aguardando assim a segunda tentativa, isso evita que robôs fiquem enviando e-mails.

VII. CONCLUSÕES

É notório que a evolução da Internet trouxe muitos benefício para a humanidade e junto, como em qualquer evolução, também trouxe problemas a serem amadurecidos e resolvidos. O e-mail é uma ferramenta essencial hoje no cotidiano de uma grande parte da população e de empresas ao redor do mundo. Devido a uma fragilidade de seu protocolo de envio, foram encontradas diversas brechas e maneiras de explorar estas conforme abordado, além das brechas encontradas no protocolo ainda temos o fator humano que quando falta informação, também influencia para que determinados ataques de spam sejam bem sucedidos. Além do fator humano a cada dia os spammers descobrem uma maneira diferente de burlar os sistemas anti-spam que estão no mercado. Portanto a melhor maneira de se proteger para não ser alvo dos spammers é saber diferenciar os e-mails comuns de spam, evitar expor os dados pessoais, e principalmente utilizar ferramentas que auxiliam na detecção e bloqueio de spam, sendo assim reduzindo a possibilidade de receber estes e-mails indesejados.

VIII. REFERÊNCIAS

- [1] Relatório de spam mensal publicado no site SpamCorp <<http://www.spamcop.net/spamstats.shtml>>. (Consultado em 22 abril 2008)
- [2] Estatísticas de Notificações de Spam Reportadas ao CERT.br <<http://www.cert.br/stats/spam/>>. (Consultado em 22 de abril 2008).
- [3] Cartilha de Segurança da Cert.br <<http://cartilha.cert.br/spam/sec1.html#subsec1.1>> (Consultado em 24 de abril de 2008).
- [4] Guia de Prevenção do antispam.br <<http://www.antispam.br>> (Consultado em 21 de abril de 2008).