Cartilha de Segurança para Internet
Parte VI: SPAM

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha aborda o conceito de SPAM e os problemas que ele pode acarretar para usuários, provedores e empresas. Também são citadas técnicas de filtragem que podem ser utilizadas por usuários para tentar bloquear o recebimento de SPAMs.

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@nic.br.

Nota de *Copyright* e Distribuição

Sumário

1 SPAM

SPAM é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial Email*).

1.1 Quais são os problemas que o SPAM pode causar para um usuário da Internet?

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, todas as mensagens enviadas a partir deste momento serão devolvidas ao remetente e o usuário não conseguirá mais receber *e-mails* até que possa liberar espaço em sua caixa postal;

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

Aumento de custos. Independentemente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do SPAM é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à Internet, cada SPAM representa 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. Como a maior parte dos SPAMs são enviados para conjuntos aleatórios de endereços de *e-mail*, não há como prever se uma mensagem com conteúdo impróprio será recebida. Os casos mais comuns são de SPAMs com conteúdo pornográfico ou de pedofilia enviados para crianças.

1.2 Quais são os problemas que o SPAM pode causar para os 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 os 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.

Perda de clientes. Os provedores muitas vezes perdem clientes que se sentem afetados pelos SPAMs que recebem ou pelo fato de terem seus *e-mails* filtrados por causa de outros clientes que estão enviando SPAM.

Investimento em pessoal e equipamentos. Para lidar com todos os problemas gerados pelo SPAM os provedores necessitam contratar mais técnicos especializados e acrescentar sistemas de filtragem de SPAM, que implicam na compra de novos equipamentos. Como conseqüência os custos do provedor aumentam.

1.3 Como fazer para filtrar os *e-mails* de modo a barrar o recebimento de SPAMs?

Existem basicamente dois tipos de *software* que podem ser utilizados para barrar SPAMs: aqueles que são colocados nos servidores, e que filtram os *e-mails* antes que cheguem até o usuário, e aqueles que são instalados nos computadores dos usuários, que filtram os *e-mails* com base em regras individuais de cada usuário.

Podem ser encontradas referências para diversas ferramentas de filtragem de *e-mails* nas páginas abaixo:

- *Spam Filters*
  http://www.paulgraham.com/filters.html
- *Free Spam Filters*
  http://wecanstopspam.org/jsp/Wiki?FreeSpamFilters
- *OpenSource Spam Filters*
  http://wecanstopspam.org/jsp/Wiki?OpenSourceSpamFilters
- *Commercial Spam Filters*
  http://wecanstopspam.org/jsp/Wiki?CommercialSpamFilters

Também é interessante consultar seu provedor de acesso, ou o administrador de sua rede, para verificar se existe algum filtro de *e-mail* instalado nos servidores que você utiliza.

1.4 Para quem devo reclamar quando receber um SPAM?

Deve-se reclamar de SPAMs para os responsáveis pela rede de onde partiu a mensagem. Se esta rede possuir uma política de uso aceitável, a pessoa que enviou o SPAM pode receber as penalidades que nela estão previstas.

Muitas vezes, porém, é difícil conhecer a real origem do SPAM. Os *spammers* costumam enviar suas mensagems através de máquinas mal configuradas, que permitem que terceiros as utilizem para enviar os *e-mails*. Se isto ocorrer, a reclamação para a rede de origem do SPAM servirá para alertar os seus responsáveis dos problemas com suas máquinas.

Além de enviar uma reclamação para os responsáveis pela rede de onde saiu a mensagem, procure manter o *e-mail* `mail-abuse@nic.br` na cópia de reclamações de SPAM. Deste modo o NBSO pode manter dados estatísticos sobre a incidência e origem de SPAMs no Brasil e, também, identificar máquinas mal configuradas que estejam sendo abusadas por *spammers*.

Vale comentar que recomenda-se não responder a um SPAM ou enviar um *e-mail* solicitando a remoção da lista. Geralmente, este é um dos métodos que os *spammers* utilizam para confirmar que um endereço de *e-mail* é válido e realmente alguém o utiliza.

Informações sobre como encontrar os responsáveis por uma rede são apresentadas na parte VI desta Cartilha: Incidentes de Segurança e Uso Abusivo da Rede.

1.5 Que informações devo incluir numa reclamação de SPAM?

Para que os responsáveis por uma rede possam identificar a origem de um SPAM é necessário que seja enviada a mensagem recebida acompanhada do seu **cabeçalho completo** (*header*).

É no cabeçalho de uma mensagem que estão as informações sobre o enderço IP de origem da mensagem, por quais servidores de *e-mail* a mensagem passou, entre outras.

Informações sobre como obter os cabeçalhos de mensagens podem ser encontradas em `http://www.antispam.org.br/header.html`.