Proposta da Comissão de Trabalho sobre Spam do Comitê Gestor da Internet no Brasil:

Tecnologias e Políticas para Combate ao Spam

Versão Preliminar

Cristine Hoepers Klaus Steding-Jessen
Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil – CERT.br

Rubens Kühl Jr.
Escola Politécnica da Universidade de São Paulo

13 de maio de 2005

Resumo

Nos últimos anos tem sido crescente a quantidade de spams circulando na Internet, bem como o número de ataques direcionados a usuários finais de Internet. Estes ataques em grande parte das vezes objetivam, além de outras finalidades, a utilização em massa de máquinas de usuários finais para envio de spams – tanto de conteúdo não solicitado, quanto relacionados com fraudes.

Neste documento são apresentadas sugestões a serem aplicadas pelas grandes operadoras de telecomunicações e provedores de acesso e conteúdo Internet, com o intuito de reduzir o número de spams e abusos partindo de redes brasileiras.

Sumário

1 Introdução

A Comissão de Trabalho sobre Spam do Comitê Gestor da Internet no Brasil tem como um de seus objetivos estudar soluções tecnológicas e operacionais para o problema do spam e propor recomendações de procedimentos operacionais e de segurança de redes que possam colaborar para a redução do spam nas redes ligadas à Internet no Brasil.

Este documento reúne um conjunto de recomendações técnicas e operacionais de combate ao spam. Estas recomendações serão discutidas e estudadas em conjunto com a comunidade Internet no Brasil, de modo a servir de base para um esforço conjunto de combate ao spam e aos incidentes de segurança que podem decorrer de seu envio.

2 Motivação

Nos últimos anos tem se observado uma grande tendência de crescimento no volume de spams na Internet, assim como também tem crescido o uso do spam na propagação de vírus/*worms* e em atividades relacionadas com fraudes (como *phishing scam*).

Um dos fatores que tem contribuído grandemente para esse cenário tem sido o anonimato provido através do abuso de computadores mal configurados de usuários finais, principalmente daqueles conectados via banda larga.

Existem diversas maneiras pelas quais os *spammers* (ou invasores em geral) podem abusar dos computadores pessoais, entre elas:

- através do acesso a *backdoors* instalados por *worms* ou *bots*;
- pela utilização de computadores com *proxies* abertos, ou seja, com o serviço *proxy* mal configurado, permitindo que qualquer pessoa conectada à Internet o utilize;
- através da instalação, sem o conhecimento do usuário, de serviços de *proxy*. Isto pode ser feito através da instalação involuntária de um cavalo de tróia pelo usuário, ou através de *worms* ou *bots*.

Uma vez que o *spammer* (ou o invasor) tenha acesso a uma máquina, ele pode realizar diversas atividades abusivas, entre elas:

- envio de spam diretamente da máquina comprometida;
- envio de spam através de um *proxy* aberto, ou através do encadeamento de sucessivos *proxies* abertos;
- utilização da máquina para realização de ataques de DDoS, com a possibilidade desta ser ativada remotamente;
- furto de informações contidas na máquina.

A facilidade com que é possível obter listas de *proxies* abertos, ou mesmo de *botnets*, tem contribuído para o aumento no número de ataques de *worms* e de fraudes ocorridas via Internet[1].

Outro grande problema é a contratação, por *spammers*, de serviços de banda larga, conectividade e hospedagem de páginas referenciadas em spams. Muitas vezes esse serviço não é contratado diretamente por um *spammer*, mas sim sublocado tanto para *spammers* nacionais quanto internacionais.

[1] "Fraudes pela Internet crescem 577% em 2004", Fonte: http://www.cert.br/docs/releases/2005/2005-02-03.html

Considerando este cenário é de interesse de cada um que sua rede não seja incluída em listas de bloqueio nem utilizada para a propagação de spams, fraudes, *worms*/vírus e contaminação por *bots* utilizados para desferir ataques de DDoS. Para que seja possível reduzir o número de spams na Internet é necessária a adoção não só de soluções técnicas, mas também de boas práticas e políticas que tratem dessa questão.

3 Recomendações para Operadoras de Telecomunicações

3.1 Fechar *proxies* abertos

Problema: *Proxies* abertos permitem o uso da conexão do cliente por *spammers* e fraudadores de forma anônima, o que muito dificulta o bloqueio e rastreio desses abusos. *Proxies* abertos comumente também participam de outros incidentes de segurança.

Recomendação: Uma combinação apropriada das seguintes medidas deve ser adotada:

- Filtros em nível de rede, impedindo a conexão em portas típicas de *proxy*;
- Varredura proativa dos clientes buscando *proxies* abertos;
- Monitoração estatística de tráfego (fluxos) em portas normalmente utilizadas em serviços de *proxy*, *e-mail* e *backdoors*;
- Monitoração dos mecanismos de notificação de abusos (vide seção 5.1);
- Ação célere e efetiva junto ao usuário quando quaisquer dos 3 últimos mecanismos acima apontar para a presença de um *proxy* aberto ou uma máquina comprometida.

3.2 Impedir envio direto de mensagens eletrônicas

Problema: Não há distinção, no protocolo SMTP, entre servidores de correio e usuários de correio, permitindo que uma máquina de usuário faça entregas de mensagens diretamente aos servidores dos destinatários. Essa técnica é normalmente empregada por *spammers* ao utilizar *proxies* abertos ou máquinas comprometidas, assim como por vírus e *worms*.

Recomendação: Deve ser eliminada a possibilidade de conexão direta entre clientes cujo perfil não preveja a operação de servidores de *e-mail* e servidores SMTP na porta 25 (caso típico de usuários domésticos). Isso força o uso de servidores de *relay* dos provedores conveniados ao serviço, das operadoras de telecomunicações ou de serviços externos autenticados, que se daria através da porta 587 (*Mail Submission Port* [1]) ou outra porta não padrão para correio definida por cada serviço. O atendimento desta recomendação depende da disponibilização de porta diferente da 25 para envio de *e-mail*, como descrito na seção 4.1.

4 Recomendações para Provedores de Correio Eletrônico

4.1 Implementar SMTP autenticado

Problema: *Spammers*, vírus ou *worms* utilizando máquinas comprometidas de usuários podem se aproveitar da capacidade de envio de correio sem necessidade de autenticação. O não atrelamento da origem da mensagem, como aparece no cabeçalho e no corpo, com o remetente, torna mais difícil o rastreio de abusos do serviço.

Recomendação: O envio de mensagens através de um servidor de correio deve ser autorizado apenas para usuários devidamente identificados no sistema, tipicamente através de autenticação por usuário e senha (SMTP AUTH [2]).

O serviço autenticado deve ser provido em porta diferente da 25, tal como a 587 (Mail Submission [3]), e os usuários instruídos a configurarem seus programas de correio para utilização dessa porta. Qualquer serviço SMTP que não o de porta 25 deve exigir autenticação.

Sugere-se que a autenticação informada seja adicionada à mensagem que será enviada (a própria linha "`Received:`" é o lugar mais seguro para isto), facilitando o trabalho da equipe de tratamento de abusos ao receber notificações.

4.2 Limitar a vazão de envio de *e-mails*

Problema: A popularização e o aumento na eficiência dos softwares de *bulk mailing* torna extremamente fácil o envio de um número altíssimo de *e-mails* pelos *spammers*. Além disso, um grande número de máquinas, comprometidas via *worms*/*bots*, também tem sido utilizado para o envio de uma quantidade enorme de spam.

Adicionalmente, o *e-mail* tem funcionado como meio de propagação de muitos vírus/*worms*, bem como meio para realização de fraudes em geral. Ambos os casos exigem, para serem bem sucedidos, o envio de uma quantidade abusiva de mensagens.

Recomendação: Provedores de correio eletrônico devem limitar a vazão de envio de *e-mails* através de seus servidores de SMTP, mantendo uma contagem do número total de destinatários associados a um mesmo remetente, por unidade de tempo. Tipicamemnte essa contagem leva em conta os campos "`To:`", "`Cc:`" ou "`Bcc:`".

Cada provedor de correio eletrônico deve determinar os seus próprios valores de vazão máxima para não prejudicar o envio legítimo de *e-mails* de seus usuários. A idéia, contudo, é impedir que um único *spammer* ou máquina comprometida envie milhões de *e-mails* por dia.

4.3 Corrigir *relays* abertos

Problema: Um *relay* é uma funcionalidade do serviço SMTP que permite receber *e-mails* de clientes e re-transmití-los para outro servidor SMTP. Máquinas com *relays* mal configurados podem ser utilizadas indiscriminadamente por terceiros para enviar spam, dificultando a identificação da real origem.

Recomendação: Servidores de SMTP devem ser configurados corretamente e testados de modo a assegurar que não estejam atuando como *relays* abertos.

4.4 Restringir a criação automática de contas

Problema: *Spammers* tem utilizado mecanismos automatizados para criação de um número enorme de contas de *e-mail* em provedores de correio eletrônico, especialmente provedores gratuitos. Essas contas são então utilizadas para o envio de uma grande quantidade de *e-mails*, incluindo spam e mensagens ligadas a fraudes em geral. Adicionalmente, muitas dessas contas podem ser utilizadas também para receber os dados capturados através de cavalos de tróia instalados nas máquinas das vítimas de fraude.

Recomendação: Provedores de correio eletrônico devem implementar métodos para impedir a criação automatizada de contas. Esses métodos podem incluir, por exemplo, testes que tentam assegurar que quem está criando a conta é realmente uma pessoa e não um programa. Provedores pagos podem exigir também algum tipo de comprovação de pagamento antes de liberar o uso da conta.

4.5 Promover mecanismos de combate à falsificação de *e-mails*

Problema: É prática comum de vírus e *worms* enviar mensagens com remetente falso. Fraudadores também fazem isso, apesar de tipicamente poderem alcançar o mesmo efeito através de remetentes verdadeiros

que lembrem as organizações pelas quais eles querem se passar. *Spammers* usualmente acabam incorrendo em remetente falso ao tentarem evitar bloqueio por remetente de seus spams.

Recomendação: Sugere-se que os provedores de correio publiquem registros públicos que permitam a validação, por outros servidores de correio, de mensagens enviadas. Tal validação pode ser de quais são os endereços IP dos servidores autorizados a enviar *e-mails* em nome de um certo domínio (tais como registros SPF [4]) e/ou de quais são as chaves públicas que assinam as mensagens vindas de um certo domínio (tais como registros DomainKeys [5]).

A publicação de registros especificando IPs não tem impacto funcional sobre os servidores de correio do provedor. A adoção dessas técnicas de combate de falsificações, por parte do provedor de correio, não é requisito ou conseqüência da publicação de registros, mas sua implementação também é sugerida em prol da diminuição da propagação de vírus, *worms* e fraudes.

5 Recomendações Gerais

5.1 Implementar acompanhamento de notificações de abuso

Problema: É pratica comum na Internet o envio de notificações de spam e de abusos para endereços de *e-mail* definidos na RFC 2142 [6] e para os endereços listados em bases públicas de serviços de Whois [7], porém nem sempre essas contas existem ou são lidas.

Recomendação: Todas as redes necessitam acompanhar as notificações de abuso recebidas tanto pelos *e-mails* da RFC 2142 [6] (como `<abuse@dominio>` e `<security@dominio>`), quanto pelas contas listadas nos contatos de Whois. No caso específico dos *e-mails* listados nos contatos de Whois é recomendado que pelo menos o contato técnico do domínio seja de um profissional que tenha contato com o pessoal das equipes de segurança e abuso.

As redes que possuírem Grupos de Resposta a Incidentes de Segurança (CSIRTs – *Computer Security Incident Response Teams*) devem anunciar o endereço do grupo junto à comunidade de segurança para que seja possível encaminhar as informações diretamente para este grupo.

5.2 Implementar políticas

Problema: Muitas redes possuem entre seus clientes aqueles que oferecem serviços de envio em massa de spams ou de hospedagem de páginas referenciadas em spams.

Recomendação: Todas as redes devem possuir políticas de uso aceitável ou contratos de prestação de serviços que prevejam como uso abusivo dos recursos tanto o envio de spam quanto a hospedagem de páginas referenciadas em spams.

Glossário

Backdoor Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Bot Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploraçao de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a disferir ataques contra outros computadores, furtar dados, enviar spam, etc.

Botnets Redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de spam, etc.

Cavalo de Tróia
Programa, normalmente recebido como um presente (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem conhecimento do usuário.

Código Malicioso
Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, *rootkits*, etc.

DDoS Do Inglês *Distributed Denial of Service*. Ataque de negação de serviço distribuído, ou seja, um conjunto de computadores utilizado para tirar de operação um ou mais serviços ou computadores conectados Internet. Veja Negação de Serviço.

DoS Do Inglês *Denial of Service*. Veja Negação de Serviço.

Negação de Serviço
Atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

Phishing Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Proxy Um servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. Proxies mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar spam.

Spam 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*)

Spammer Pessoa que envia spam.

Vírus Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Vulnerabilidade
: Falha no projeto, implementação ou configuração de um software ou sistema operacional, que quando explorada por um atacante resulta na violação da segurança de um computador.

Worm
: Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros progamas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Referências

[1] R. Gellens and J. Klensin, "RFC 2476: Message Submission." http://www.ietf.org/rfc/rfc2476.txt, 1998 December.

[2] J. Myers, "RFC 2554: SMTP Service Extension for Authentication." http://www.ietf.org/rfc/rfc2554.txt, March 1999.

[3] C. Hutzler, D. Crocker, P. Resnick, and R. Sanders, "Draft: Email Submission Between Independent Networks." http://www.ietf.org/internet-drafts/draft-hutzler-spamops-04.txt, May 2005.

[4] M. Wong and W. Schlitt, "Draft: Sender Policy Framework: Authorizing Use of Domains in E-MAIL." http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-02.txt, June 2005.

[5] M. Delany, "Draft: Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)." http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-02.txt, March 2005.

[6] D. Crocker, "RFC 2142: Mailbox Names for Common Services, Roles and Functions." http://www.ietf.org/rfc/rfc2142.txt, May 1997.

[7] K. Harrenstien, M. Stahl, and E. Feinler, "RFC 954: NICNAME/WHOIS." http://www.ietf.org/rfc/rfc954.txt, October 1985.

[8] J. Postel, "RFC 821: Simple Mail Transfer Protocol." http://www.ietf.org/rfc/rfc821.txt, August 1982.

[9] J. Klensin, "RFC 2821: Simple Mail Transfer Protocol." http://www.ietf.org/rfc/rfc2821.txt, April 2001.

[10] P. Hoffman, "RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security." http://www.ietf.org/rfc/rfc3207.txt, February 2002.

[11] Comitê Gestor da Internet no Brasil, "Recomendações para o Desenvolvimento e Operação da Internet no Brasil." http://www.cgi.br/infoteca/documentacao/desenvolvimento.htm, Agosto 1999.

[12] Anti-Spam Technical Alliance, "Anti-Spam Technical Alliance Technology and Policy Proposal." http://postmaster.info.aol.com/asta/proposal.html, June 2004.