Gerência de Porta 25: Motivação, Importância da Adoção para o Combate ao Spam e Discussões no Brasil e no Mundo

Cristine Hoepers Klaus Steding-Jessen
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR

Versão 1.2 – 27/01/2009

Sumário

1 Introdução

O *spam* é uma das formas de abuso da Internet que mais tem crescido, atualmente sendo responsável por uma parcela significativa dos *emails* que trafegam na rede [1, 2]. Além disso, o *spam* tem sido amplamente utilizado para enviar mensagens relacionadas com *phishing* (mensagem que procura induzir usuários ao fornecimento de dados pessoais e financeiros) e para disseminação de códigos maliciosos [3].

Existe, também, um aumento da sofisticação dos *softwares* de envio de *spam*, o que torna as técnicas existentes de bloqueio ainda menos eficientes e a rastreabilidade do *spammer* (remetente do *spam*) mais difícil [4,

3]. Um exemplo disso é o crescimento na utilização de máquinas infectadas por códigos maliciosos, como os *bots* (programas que, além de serem capazes de se propagar através da exploração de vulnerabilidades em computadores, podem ser controlados remotamente por um invasor), para o envio de *spam* e *phishing* [3], permitindo que o *spammer* permaneça no anonimato. Máquinas com *proxies* abertos são abusadas de maneira similar, como ficou evidente nos resultados do Projeto SpamPots [5].

Este documento discute um conjunto de políticas e padrões, comumente chamados de "Gerência de Porta 25", para a mitigação do abuso de *proxies* abertos para o envio de *spam* e para aumentar a rastreabilidade de fraudadores e *spammers*. Estes padrões, que procuram diferenciar a submissão do transporte de *emails*, já foram avaliados pela comunidade Internet, estão em discussão no Brasil desde 2005 e já são utilizados em redes de banda larga de caráter residencial de diversos países.

2 O Problema do Abuso de *Proxies* Abertos e do Envio de *Spam* por Máquinas Infectadas

Um *proxy* é um servidor que atua como intermediário entre um cliente e outro servidor, ou seja, um serviço de *proxy* faz conexões em nome de outros clientes [6]. Quando um *proxy* está mal configurado, ele permite o redirecionamento indiscriminado de conexões de terceiros para quaisquer endereços IP e portas, sendo denominado *proxy* aberto. *Proxies* abertos são também intencionalmente instalados por códigos maliciosos, como *bots* e cavalos-de-tróia. Os *spammers* utilizam estes *proxies* abertos para efetuar conexões para os servidores SMTP dos destinatários do *spam*, de forma a obter anonimato [7, 8].

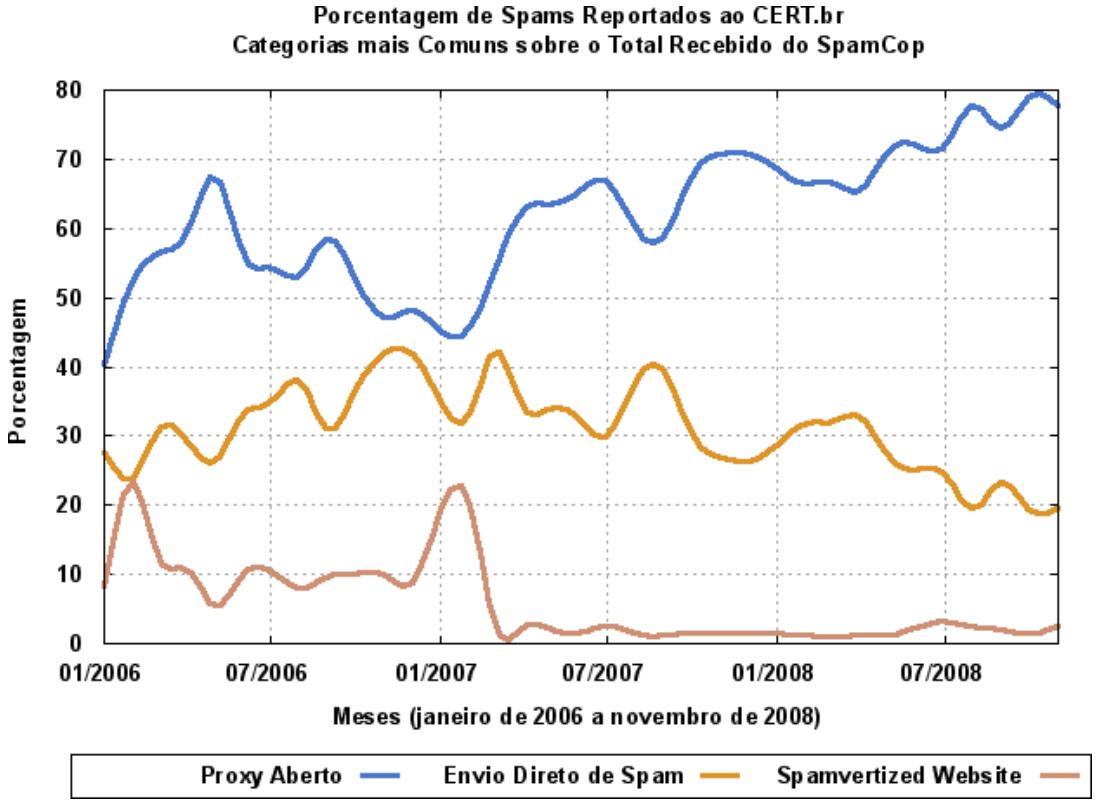

Figura 1: Distribuição das reclamações de *spam* mais comuns entre janeiro de 2006 e novembro de 2008.

Nas reclamações de *spams* originados no Brasil, enviadas ao CERT.br pela entidade *SpamCop* (que somaram cerca de meio milhão somente no último trimestre), a maioria absoluta é de abuso de *proxies* instalados em

máquinas conectadas via banda larga.

A Figura 1 evidencia que as reclamações relativas a abuso de *proxies* têm sido, historicamente, o maior problema das redes no Brasil. Seguido do envio direto de mensagens, provavelmente através de máquinas infectadas por códigos maliciosos, como os *spambots*. Esta entrega direta de mensagens ocorre quando o envio é feito, por um cliente, diretamente para o servidor de *e-mails* do destinatário, subvertendo o processo de submissão de mensagens via um servidor SMTP.

Este cenário é preocupante, pois o abuso das máquinas com *proxies* abertos traz, entre outras, as seguintes conseqüências:

- Utilização indevida da banda das operadoras sendo abusadas. Na seção 2.1 são apresentados alguns números sobre o consumo de banda nacional por *spammers* de fora do país;
- Utilização indevida dos recursos do usuário. Um dos maiores reflexos para os usuários sendo abusados é a lentidão da conexão com a Internet e o consumo de recursos de seu computador por *spammers*.

2.1 Resultados do Projeto SpamPots

O CGI.br, através da Comissão de Trabalho Anti-spam (CT-Spam), patrocinou o Projeto SpamPots. Coordenado e desenvolvido pelo CERT.br, do NIC.br, foi uma iniciativa pioneira que utilizou *honeypots* de baixa interatividade na obtenção de métricas sobre o abuso de redes de banda larga para o envio de *spam* [5]. A arquitetura contou com 10 *honeypots* de baixa interatividade instalados em redes brasileiras de banda larga de 5 operadoras diferentes (cabo e ADSL). Os *honeypots* permaneceram instalados em 4 cidades brasileiras por um período de 15 meses.

Estes *honeypots* foram configurados de modo a simular computadores com *proxies* abertos. Desse modo, um *spammer* que tentasse abusar de um destes honeypots para o envio de *spam*, seria levado a acreditar que teve sucesso em enviar seus *emails*. Porém, as mensagens não eram entregues, mas apenas armazenadas para posterior análise.

Neste período, em apenas 10 máquinas de banda larga, foram injetados mais de meio bilhão de e-mails, que seriam entregues a mais de 4 bilhões de destinatários. Isso significa que apenas 10 máquinas sendo abusadas em uma rede de banda larga enviam, por dia, cerca de 9 milhões de *spams*. A Tabela 1 apresenta os números gerais do período.

Tabela 1: Estatísticas gerais referentes aos *emails* capturados.

Início da coleta dos dados	10/06/2006
Fim da coleta dos dados	18/09/2007
Dias de dados coletados	466
Total de emails coletados	524.585.779
Total de destinatários	4.805.521.964
Média de destinatários por *spam*	9,16
Média de emails por dia	1.125.720
IPs únicos que enviaram *spam*	216.888
ASs únicos que enviaram *spam*	3.006
Países (country codes) de origem	165

Foi observada uma grande concentração nos países de origem dos *spams*. De todo o *spam* que foi capturado pelo projeto, 97% foi originado em apenas 5 países: Taiwan, China, Estados Unidos, Canadá e Japão. Como

resultado do processo de *data mining* das mensagens, observou-se que 94% dos *spams* tinham como destino outros países, e não o Brasil.

Este fato deixa claro que, não só os *spammers* estão consumindo a banda dos usuários, como também estão consumindo banda internacional, pois todo o tráfego se origina de e se destina a outros países.

3 O que é Gerência de Porta 25

A gerência de porta 25 é o nome dado ao conjunto de políticas e tecnologias, implantadas em redes de usuários finais ou de caráter residencial, que procura separar as funcionalidades de submissão de mensagens, daquelas de transporte de mensagens entre servidores.

A definição do padrão para o protocolo de submissão é de 1998, sendo sua última revisão de 2006 [9]. Este protocolo, chamado de "*Message Submission*" fornece um meio para distinguir uma submissão do transporte de mensagens, permitindo assim:

- a aplicação de políticas diferentes para cada tipo de conexão, impedindo *relays* não autorizados ou introdução de *emails* não solicitados;
- a implementação de autenticação na submissão, incluindo aquela realizada remotamente por usuários autorizados;
- a possibilidade de implementar, futuramente, melhorias no serviço de submissão.

A adoção do protocolo de *Message Submission* é uma boa prática reforçada na RFC 5068 (BCP 134) [10] e que tem sido recomendada por diversos fóruns de combate ao *spam*, como o *Messaging Anti-Abuse Working Group* (MAAWG)[1], o *London Action Plan*[2] e a própria CT-Spam [11], do CGI.br.

No documento *Managing Port 25 for Residential or Dynamic IP Space – Benefits of Adoption and Risks of Inaction* [12] o MAAWG recomenda para redes de caráter residencial, além da adoção de *Message Submission*, as seguintes medidas:

- requerer autenticação para a submissão de mensagens, como recomendado na RFC 4954 [13];
- configurar o *software* cliente de *email* para usar porta 587/TCP[3] e autenticação;
- não interferir no tráfego para a porta 587/TCP[4];
- bloquear acesso de saída para porta 25/TCP a partir de todas as máquinas que não sejam MTAs ou explicitamente autorizadas.

3.1 Benefícios

A adoção de gerência de porta 25 pode trazer diversos benefícios para as operadoras que as implementarem. A seguir são listados alguns dos benefícios mais imediatos da adoção.

[1] http://www.maawg.org/

[2] http://www.londonactionplan.org/

[3] No primeiro *draft* do SSL v3.0, a Netscape recomendava a utilização da porta 465/TCP para submissão de mensagens via SMTPS. O uso desta porta para submissão de mensagens é *deprecated* e nunca tornou-se um padrão na Internet. Mesmo assim, muitos *softwares* clientes de *e-mail* e alguns servidores de submissão, ainda utilizam esta porta.

[4] Apesar de não constar explicitamente na recomendação do MAAWG, é importante que também não ocorra interferência no tráfego relacionado com outras portas que possam ser utilizadas para submissão, como a 80/TCP ou a 465/TCP.

- Saída dos blocos das operadoras de listas de bloqueio – com a diferenciação das conexões de perfil residencial, daquelas de perfil comercial, e a redução dos *spams* enviados, este é um dos primeiros reflexos.
- Diminuição de reclamações de usuários – com suas máquinas não sendo mais abusadas, o usuário sente uma sensível diminuição no uso dos recursos computacionais, bem como, com a redução do consumo de banda para envio de *spam*, ele sente melhores condições de utilização da rede.
- Dificulta o abuso da infra-estrutura da Internet para atividades ilícitas (fraudes, furto de dados, etc).
- Aumento de rastreabilidade em caso de abuso.
- Atua na submissão, antes da mensagem entrar na infra-estrutura de *e-mail*, implicando em menos desperdício de banda e em menos esforço de configuração de filtros anti-spam.
- Diminuição do consumo de banda internacional por *spammers* – como mostram os resultados do Projeto SpamPots, 99.84% das conexões eram originadas do exterior e mais de 90% dos *spams* eram destinados a redes de outros países.
- Diminuição de custos operacionais – o *spam* foi o mais apontado como responsável pela demanda de recursos operacionais no "*2008 Worldwide Infrastructure Security Report*" (http://www.arbornetworks.com/report).

3.2 Quem Adota no Mundo

As recomendações de gerência de porta 25/TCP já são adotadas por diversos membros do MAAWG, incluindo Earthlink, AOL e Comcast. No caso da Comcast, após a adoção da medida, o número de *spams* barrados diariamente na saída de sua rede chegava a cerca de 700 milhões [14]. Algumas referências *on-line* sobre a implementação desta prática nos Estados Unidos são as que seguem:

- *Earthlink blocks port 25 outgoing!, Oct 2000*
  http://www.broadbandreports.com/shownews/492
- *Blocking Port 25 Traffic – 'MyDoom' virus reheats the discussion, Jan 2004*
  http://www.broadbandreports.com/shownews/38004
- *Comcast takes hard line against spam, Jun 2004*
  http://news.zdnet.com/2100-3513_22-5230615.html
- *Providers That Block Port 25: NetZero, Mindspring, MSN, Earthlink, Flashnet, MediaOne, AT&T, Verizon, BellSympatico*
  http://kb.earthlink.net/case.asp?article=resid9226

De modo similar, há diversos outros casos de implantação de gerência de porta 25 para reduzir o abuso de redes por *spammers*. Seguem alguns exemplos:

- No Brasil, a Sercomtel, operadora de Londrina/PR, já implementou. Um estudo de caso da implantação foi apresentado no evento GTS-9, em Belo Horizonte/MG, em 30 de junho de 2007.
  ftp://ftp.registro.br/pub/gts/gts09/06-mail-submission.pdf
  ftp://ftp.registro.br/pub/gter/gter23/videos/mp4/gts-06-mail-submission.mp4

- Segundo resultados do "*Survey on Providers' Security and Anti-Spam Measures*", realizado pela ENISA (*European Network and Information Security Agency*), 50% dos ISPs Europeus consultados já implementam.
  http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf
- Na Suíça, a S.I.A.S. (*Swiss ISPs Against Spam*) recomenda a prática, já adotada por: Bluewin, cablecom e green.ch.
  http://www.stopspam.ch/engl/infos.htm
- No Japão a recomendação do JEAG (*Japan Email Anti-Abuse Group*) existe desde 2006.
  http://jeag.jp/

4 Discussões sobre o Assunto no Brasil

No cenário brasileiro, a implementação da gerência de porta 25 depende do trabalho coordenado de 2 setores:

- As empresas que fornecem serviços de conectividade, através de banda larga de caráter residencial ou *dial-up*. Sendo estes, responsáveis pelo bloqueio de saída de tráfego na porta 25/TCP, em redes com as características citadas, e não interferência no tráfego da porta 587/TCP ou de qualquer outra utilizada para submissão de mensagens;
- Os provedores de acesso à Internet, que fornecem as contas de *e-mail* aos usuários. Sendo estes, responsáveis por prover serviço de submissão de mensagens, com autenticação, em porta diferente da 25/TCP (via *Message Submission* ou *Webmail*).

Dado este caráter de cooperação, a CT-Spam vem discutindo este assunto com a comunidade Internet brasileira desde 2005. São de destaque as seguintes atividades realizadas:

Maio/2005 – Publicação do documento "Tecnologias e Políticas para Combate ao *Spam*" [11].

Junho/2005 – Reunião com Operadoras e Provedores para discussão e apresentação do documento.

Dezembro/2005 – Apresentação e discussão da proposta na CBC-1 (Comissão Brasileira de Telecomunicações – Segurança das Telecomunicações) da Anatel.

2006/2007 – Desenvolvimento e operação do Projeto SpamPots, para um melhor entendimento do abuso das redes brasileiras e a determinação de mitigações mais efetivas.

Junho e Setembro/2007 – Reuniões entre o CERT.br, Operadoras de Banda Larga e CSIRTs de Instituições Financeiras, para discussão do abuso de redes residenciais para o envio de *spam* e *phishing*.

Novembro/2007 – Reuniões entre o CERT.br, Operadoras de Banda Larga, Provedores de Acesso à Internet e CSIRTs de Instituições Financeiras, para discussão do abuso de redes residenciais para o envio de *spam* e *phishing*.

Fevereiro/2008 – Discussão na CBC-1 Anatel sobre gerência de porta 25/TCP em conexões residenciais, controle de *direct delivery* e adoção de *message submission*.

Dezembro/2008 – Reunião da CT-Spam com operadoras de banda larga, provedores de acesso e associações representantes de provedores de acesso e operadoras de telefonia fixa, para discussão dos benefícios e impactos da adoção da gerência de porta 25 em redes de perfil residencial, no Brasil.

5 Histórico de Revisões

Versão 1.0 – 13/11/2008: Versão Inicial.

Versão 1.1 – 23/12/2008: Revisão de erros de digitação; inclusão da seção sobre benefícios e de novas referências sobre a implantação no Brasil e no mundo; inclusão de observações específicas sobre outras portas que podem vir a ser usadas para submissão de mensagens.

Versão 1.2 – 27/01/2009: Revisão de erros de digitação.

Referências

[1] B. Hayes, "Spam, spam, spam, lovely spam," *American Scientist*, vol. 91, pp. 200–204, May–June 2003.

[2] Messaging Anti-Abuse Working Group (MAAWG), "Email Metrics Reports." http://www.maawg.org/about/EMR/, 2007.

[3] J. Milletary, "Technical trends in phishing attacks." http://www.cert.org/archive/pdf/Phishing_trends.pdf, October 2005. CERT Coordination Center, Carnegie Mellon University.

[4] L. F. Cranor and B. A. LaMacchia, "Spam!," *Commun. ACM*, vol. 41, no. 8, pp. 74–83, 1998.

[5] CERT.br, "Resultados Preliminares do Projeto SpamPots: Uso de Honeypots de Baixa Interatividade na Obtenção de Métricas sobre o Abuso de Redes de Banda Larga para o Envio de Spam." http://www.cert.br/docs/whitepapers/spampots/, Setembro 2007.

[6] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "RFC 2616: Hypertext Transfer Protocol – HTTP/1.1." http://www.ietf.org/rfc/rfc2616.txt, June 1999.

[7] A. Chuvakin, "Honeynets: High Value Security Data – Analysis of real attacks launched at a honeypot," *Elsevier Network Security*, vol. 2003, pp. 11–15, August 2003. ISSN: 1353-4858.

[8] N. Krawetz, "Anti-honeypot technology," *IEEE Security & Privacy*, vol. 2, pp. 76–79, January–February 2004.

[9] R. Gellens and J. Klensin, "RFC 4409: Message Submission for Mail." http://www.ietf.org/rfc/rfc4409.txt, April 2006.

[10] C. Hutzler, D. Crocker, P. Resnick, E. Allman, and T. Finch, "RFC 5068: Email Submission Operations: Access and Accountability Requirements." http://www.ietf.org/rfc/rfc5068.txt, November 2007.

[11] C. Hoepers, K. Steding-Jessen, and R. K. Junior, "Tecnologias e políticas para combate ao spam." http://www.cert.br/docs/ct-spam/ct-spam-tecnologias-politicas.pdf, Feb 2008.

[12] Messaging Anti-Abuse Working Group (MAAWG), "Managing Port 25 for Residential or Dynamic IP Space – Benefits of Adoption and Risks of Inaction." http://www.maawg.org/port25/MAAWG_Port25rec0511.pdf, Dec 2005.

[13] R. Siemborski, Ed., and E. A. Melnikov, "RFC 4954: SMTP Service Extension for Authentication." http://www.ietf.org/rfc/rfc4954.txt, July 2007.

[14] R. Kolstad, "The Only Good Spam Comes from Hormel," *;login:*, vol. 30, pp. 2–3, February 2005. http://www.usenix.org/publications/login/2005-02/openpdfs/motd.pdf.