UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

GIOVANI COLOMBO

ESTUDO E IMPLEMENTAÇÃO DO GERENCIAMENTO DA PORTA 25 (SMTP) NA COPEL TELECOMUNICAÇÕES

MONOGRAFIA

CURITIBA
2013

GIOVANI COLOMBO

ESTUDO E IMPLEMENTAÇÃO DO GERENCIAMENTO DA PORTA 25 (SMTP) NA COPEL TELECOMUNICAÇÕES

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTF-PR.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2013

Aos meus pais, Divercino e Águida (*in memorian*), minha irmã Giane, minha esposa Wrenely, meu avô Reinaldo (*in memorian*), minha enteada Jennifer e seu esposo Rodrigo e meu neto Joseph.

Ao Prof. Dr. Ivan Eidt Colling, meu orientador e professor no curso de Engenharia Elétrica pela sua dedicação em ensinar e compartilhar o seu conhecimento.

Aos amigos e colegas Joelson Tadeu Vendramin e Fábio Manosso Alvariz pelo incentivo e compartilhar seus conhecimentos sobre redes de computadores.

À UTFPR, que me proporcionou uma formação profissional como Técnico em Eletrotécnica (CEFET-PR), Engenheiro Eletricista e Segurança do Trabalho.

AGRADECIMENTOS

Ao Prof. Dr. Agusto Foronda por sua dedicação e orientação neste trabalho.

Aos colegas da Copel Telecomunicações, envolvidos diretamente no gerenciamento da porta 25 que contribuíram para alcançar os resultados obtidos.

RESUMO

COLOMBO, Giovani. **Estudo e implementação do gerenciamento da porta 25 (SMTP) na Copel Telecomunicações**. 2013. 47 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

A presente monografia apresenta o estudo para a implementação do gerenciamento da porta 25 (SMTP) na Copel Telecomunicações através da aplicação de filtro bloqueando a porta 25 dos IPs da Copel Telecomunicações, utilizando-se da informações obtidas em *blacklists*. A vantagem desse procedimento é proteger a faixa de IPs, diminuir o número de *spams* e os clientes podem enviar seus *e-mails* com a certeza de não serem listados.

Palavras-chave: Redes, Correio eletrônico, e-mail, SMTP, Porta 25, *spam*, *Blacklist*.

ABSTRACT

COLOMBO, Giovani. **Estudo e implementação do gerenciamento da porta 25 (SMTP) na Copel Telecomunicações**. 2013. 47 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

This monograph presents the study for the implementation of the management port 25 (SMTP) on Copel Telecommunications by applying filter blocking port 25 of the IPs of Copel Telecommunications, using the information obtained from blacklists. The advantage of this procedure is to protect the IP range, decrease the number of spam and clients can send your emails to make sure they are not listed.

Keywords: Network, Electronic mail, e-mail, SMTP, Port 25, spam, Blacklist.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ACL	-	*Access Control Lists*
ANATEL	-	Agência Nacional de Telecomunicações
ARPA	-	*Advanced Research Projects Agency*
ASCII	-	*American Standard Code for Information Interchange*
ASN	-	*Autonomous System Number*
BEL	-	Banda Extra Larga
BGP	-	*Border Gateway Protocol*
CBL	-	*Composite Blocking List*
CERT.br	-	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	-	Comitê Gestor da Internet no Brasil
CIDR	-	*Classless Inter-Domain Routing*
COPEL	-	Companhia Paranaense de Energia
CRLF	-	*Carriage Return Line Feed*
DEC	-	*Digital Equipment Corporation*
DNS	-	*Domain Name System*
EDD	-	*Ethernet Demarcation Device*
EUA	-	Estados Unidos da América
FTP	-	*File Transfer Protocol*
HTTP	-	*Hypertext Transfer Protocol*
ICF	-	*Inner City Fund*
IETF	-	*The Internet Engineering Task Force*
IMAP	-	*Internet Message Access Protocol*
IP	-	*Internet Protocol*
MIT	-	*Massachusetts Institute of Technology*
MTA	-	*Mail Transfer Agent*

MUA	-	*Mail User Agent*
OS	-	Ordem de Serviço
POP3	-	*Post Office Protocol* versão 3
RBLs	-	*Realtime Blackhole Lists*
Registro.br	-	Registro de Domínios para a Internet no Brasil
RFC	-	*Request for Comments*
SMTP	-	*Simple Mail Transfer Protocol*
TCP	-	*Transmission Control Protocol*
TI	-	Tecnologia da Informação
UBE	-	*Unsolicited Bulk E-mail*
UCE	-	*Unsolicited Comercial E-mail*
USENET	-	*Unix User Network*
WWW	-	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

No início dos anos 90, a sociedade brasileira conheceu uma revolução tecnológica na área das comunicações de dados através da internet (como conhecemos hoje), que agregou vários serviços como *World Wide Web* (WWW), transferência de arquivos (*FTP – File Transfer Protocol*), acesso via terminal remoto (TELNET) e o foco deste trabalho o correio eletrônico (*e-mail*). (CARVALHO, 2006).

Em 1965, o *Massachusetts Institute of Technology* (MIT) enviou a primeira mensagem eletrônica e estabeleceu as bases para a primeira padronização (RFC 733 – *Standard for the format of ARPA Network text messages*) em 1977. (IDGNOW!, 2013a).

Para o envio e recebimento de uma mensagem eletrônica da origem para um destino (Figura 1) necessitam-se de alguns protocolos chamados: *Simple Mail Transfer Protocol* (SMTP), *Post Office Protocol* versão 3 (POP3) e *Internet Message Access Protocol* (IMAP).

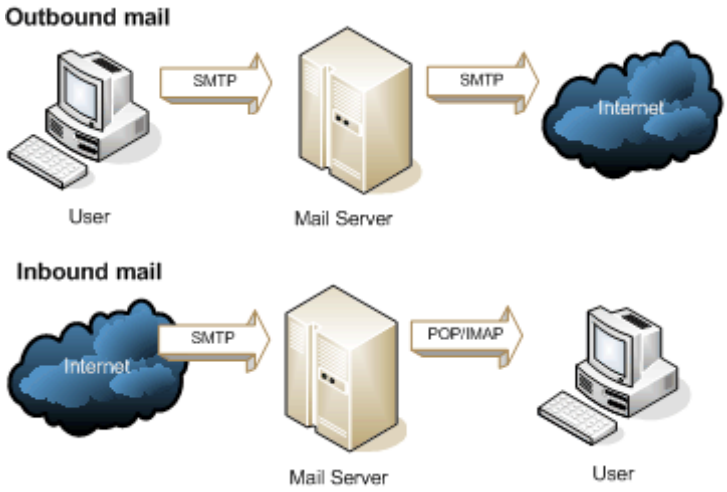


Figura 1 - Protocolos envolvidos numa transmissão/recepção de um *e-mail.*
Fonte: http://goo.gl/wBzSE

Observa-se que a submissão do *e-mail* através do cliente-servidor e do servidor-servidor utiliza-se do mesmo protocolo SMTP. Este trabalho, restringir-se-á ao gerenciamento da porta 25 (SMTP) entre cliente-servidor.

Em 1994, dois advogados Canter e Siegel postaram uma mensagem no grupo de discussão da *Unix User Network* (USENET) fazendo propaganda sobre uma loteria de *green cards* para imigrantes nos Estados Unidos, contribuindo para a

primeira mensagem eletrônica não-solicitada (*spam*). (TEIXEIRA, 2004)

Segundo um relatório da McAfee e ICF International de 2009, informa que em 2008 foram enviados no mundo um valor estimado de 62 trilhões de *spams*. O mesmo relatório aponta que o consumo anual de energia elétrica é de 33 bilhões de quilowatts-hora (kWh), equivalendo ao consumo de 2,4 mihões de residências nos Estados Unidos da América (EUA). (McAFEE, ICF, 2013)

Em 2009, o Brasil estava em primeiro lugar no envio de mensagens eletrônicas não-solicitadas. (IDGNOW!, 2013b). Neste mesmo ano, na *blacklist* UCEPROTECT®-NETWORK (http://www.uceprotect.net/en/rblcheck.php) vários Sistemas Autônomos (*Autonomous System Number* – ASN) brasileiros apareciam entre os *TOP* 10. Atualmente, está em décimo-segundo (12º) lugar. (IDGNOW!, 2013b). E não aparecemos mais na lista TOP 10 da UCEPROTECT®-NETWORK.

No ano de 2009, o Comitê Gestor da Internet no Brasil (CGI.br) emitiu a resolução CGI.br/RES/2009/002/P – Recomendação para a adoção de Gerência de Porta 25 em Redes de Caráter Residencial que tratava sobre a implementação de mecanismos de autenticação na submissão de mensagens e restrição através do bloqueio da porta 25 para evitar a entrega direta de mensagens de máquinas de clientes. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2013).

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Em virtude da importância do combate ao *spam*, pretende-se, com o presente trabalho, apresentar o procedimento executado pela Copel Telecomunicações SA no gerenciamento através do bloqueio da porta 25 (SMTP), permitindo que somente servidores de *e-mail* possam utilizar a referida porta e exibir os resultado obtidos desde setembro de 2010.

1.1.2 Objetivos Específicos

a) revisar a literatura técnica sobre o funcionamento do correio eletrônico;
b) revisar a literatura técnica sobre o protocolo SMTP;
c) explicar sobre *spam*: definição, história, classificação, impacto e estatísticas;

d) explanar sobre o funcionamento das *blacklists*;
e) explicar o procedimento adotado para bloquear o tráfego da porta 25 (SMTP) para os clientes novos e em operação;
f) apresentar os resultados obtidos com esse procedimento adotado em setembro de 2010.

1.2 JUSTIFICATIVA

Pretende-se com esse trabalho, divulgar o procedimento adotado e os resultados obtidos pela Copel Telecomunicações SA no combate ao *spam* trazendo como benefícios à diminuição da reclamação dos clientes, das atividades ilícitas (fraudes, furtos de dados), do consumo de banda, dos custos operacionais e aumentando à satisfação dos clientes.

1.3 METODOLOGIA

A metodologia do trabalho consiste:

a) revisar a literatura técnica sobre o correio eletrônico; protocolo SMTP; as mensagens não-solicitadas e o funcionamento das *blacklists*;

b) redação da monografia;

c) preparação da apresentação.

2 REFERENCIAL TEÓRICO

2.1 INTRODUÇÃO

Neste capítulo são abordados três tópicos:

a) correio eletrônico: funcionamento do *e-mail* e o protocolo: SMTP;
b) *spam*: definição, história, classificação, impactos e estatísticas no Brasil;
c) listas negras *(blacklists)*: funcionamento geral e funcionamento específico da UCEPROTECT®-NETWORK.

2.2 CORREIO ELETRÔNICO

2.2.1 Descrição do funcionamento do *e-mail*

Das aplicações utilizadas da internet uma das mais populares é o correio eletrônico. Comparando-se com o correio normal, o correio eletrônico assemelha-se em ser assíncrono, isto é, o envio e o recebimento de mensagens não dependem da fixação de horários. Porém, as vantagens são a rapidez, a facilidade na distribuição e por ser barato. Atualmente, as mensagens podem incluir além do texto, imagens, sons, vídeos, *hiperlinks* e textos em *Hypertext Transfer Protocol* (HTTP). (KUROSE, ROSS, 2003).

As mensagens eletrônicas são enviadas de um indivíduo para outro ou grupo de indivíduos através de redes de computadores. (TEIXEIRA, 2004).

Segundo Comer (2007), o endereço eletrônico é único e dividido em duas partes: nome@domínio. Sendo que

> "[...] a primeira identifica a caixa de correio de um usuário e a segunda identifica o computador em que a caixa de correio reside. O software de *e-mail* no computador do remetente usa a segunda parte para selecionar um destino; o software de *e-mail* no computador do receptor usa a primeira parte para selecionar uma caixa de correio particular" (COMER, 2007).

O sistema de e-mail possui três componentes importantes: agentes usuários, servidores de correio e protocolos, conforme Figura 2.

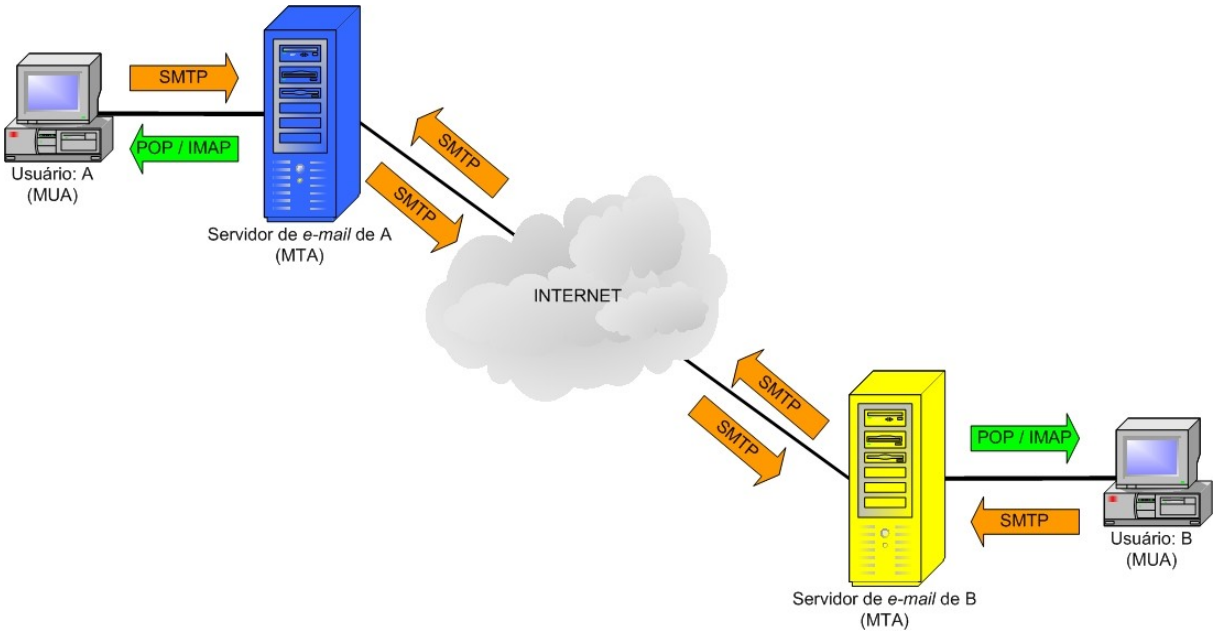


Figura 2 – Componentes do correio eletrônico: MUA, MTA e protocolos
Fonte: Própria

O *Mail User Agent* (MUA) faz a interface entre o usuário e sua caixa postal, onde estão armazenadas as mensagens eletrônicas. Diferenciam-se pelas funções disponíveis para gerenciar as caixas postais e o armazenamento das mensagens. Os principais protocolos utilizados são o POP e o IMAP. (TEIXEIRA, 2004).

O *Mail Transfer Agent* (MTA) é responsável por enviar e receber *e-mails*. Quando um *e-mail* é recebido pelo MTA, ele analisa o cabeçalho e encaminha para a caixa postal. E quando é enviada uma mensagem, ele analisa os dados e encaminha para o servidor de *e-mail* do usuário de destino. O principal protocolo utilizado é o SMTP. (TEIXEIRA, 2004).

2.2.2 Protocolo SMTP

A primeira versão do protocolo SMTP foi apresentada em novembro de 1981 com a RFC 788. Houve atualizações em agosto de 1982 (RFC 821), abril de 2001 (RFC 2821) e a última em outubro de 2008 com a RFC 5321.

O objetivo do SMTP é transportar um objeto de *e-mail* composto de um envelope e o conteúdo no formato *American Standard Code for Information Interchange* (ASCII) de 7 bits. O envelope consiste de uma série de comandos SMTP, endereço de origem e de destinatário(s) e informações adicionais do tipo da mensagem. O conteúdo é enviado pelo comando DATA e é dividido em duas partes: seção de cabeçalho e o corpo. (THE..., 2013b).

Segundo a RFC 5321, a transferência de mensagens inicia-se com o estabelecimento do canal de transmissão (*three way handshake*). Em seguida, uma série de comandos para especificar a origem e o destino (envelope) e posteriormente o conteúdo da mensagem. Para cada comando, o servidor responde na forma de um valor numérico e um texto. O código numérico é usado em programas e o texto para entendimento humano. As respostas indicam que o comando foi aceito, que comandos adicionais são esperados ou uma condição de erro temporário ou permanente existe. (THE..., 2013b).

Na Figura 3 tem-se um exemplo da sequência de comandos e respostas entre o usuário giovani@a.net.br e joseph@b.net.br com sucesso: (THE..., 2013b).

a) após o estabelecimento do canal de transmissão, o servidor responde com uma mensagem de abertura. Observa-se que foi informado o nome do servidor de destino (b.net.br);
b) cliente envia o comando EHLO indicando sua identidade (a.net.br);
c) servidor responde com 250 OK e uma saudação “Olá a.net.br, prazer em conhecê-lo”;
d) comando MAIL FROM: informa a identificação do remetente (giovani@a.net.br);
e) servidor responde com 250 OK e informa como remetente OK;
f) comando RCPT TO: identifica a caixa de correio do destino (joseph@b.net.br);
g) servidor responde com 250 OK e informa como destinatário OK;
h) comando DATA sinaliza ao servidor que enviará o conteúdo da mensagem;
i) servidor responde com 354 (start mail input; end with <CRLF . CRLF>) comece a enviar e-mail e finalize com <CRLF . CRLF>;
j) cliente envia o conteúdo da mensagem;
k) finalização da mensagem com <CRLF . CRLF>;
l) servidor responde com 250 OK (mensagem aceita para entrega);
m) após a entrega da mensagem é finalizado com o comando QUIT;
n) o servidor b.net.br responde com 221 avisando que fechará a conexão TCP estabelecida.

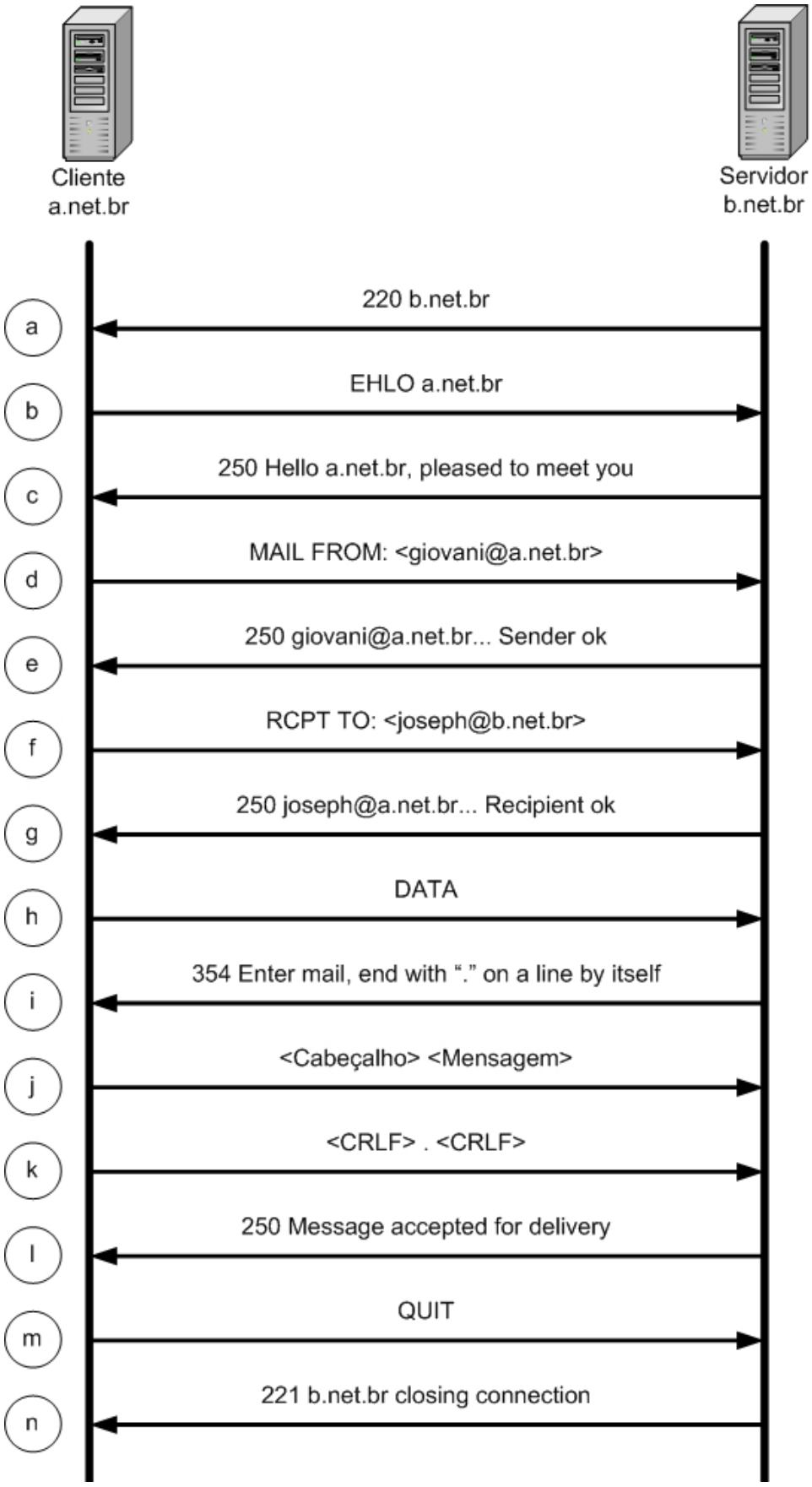


Figura 3 – Sequência de comandos e respostas para o encaminhamento de *e-mail* entre os servidores a.net.br e b.net.br.
Fonte: Própria. Adaptado (KUROSE, ROSS, 2003)

2.3 SPAM

2.3.1 Definição

Na literatura técnica existem várias definições para o termo *spam*. Para a autora Teixeira (2004), uma definição genérica seria “[...] como qualquer mensagem eletrônica não-solicitada.” (TEIXEIRA, 2004). Outra definição, adotada pela mesma autora é “toda mensagem eletrônica enviada a um ou mais usuários, sem que este(s) tenha(m) explicitamente solicitado o envio desta.” (TEIXEIRA, 2004).

No capítulo 5 da Cartilha de segurança para Internet versão 4.0 de autoria do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) expressa que “Spam é o termo usado para se referir aos e*-mails* não solicitados [...]”. (CENTRO..., 2012).

Uma definição bem completa, extraído do texto “O que é Spam?”, do Movimento Anti-spam Brasileiro é

> “No ambiente internet, *spam* significa enviar uma mensagem qualquer para qualquer quantidade de usuários, sem primeiro obter a expressa e explícita autorização daqueles destinatários. Este procedimento, propiciado pelo baixo custo de envio de mensagem eletrônica, causa inconveniência e custo para o destinatário.” (TEIXEIRA, 2004).

Os *e-mails* de *spam* também são chamados de *junk* (lixo) *e-mails* e o usuário que envia é conhecido como *spammer*. (TEIXEIRA, 2004).

Finalmente, os dois últimos termos são: (TEIXEIRA, 2004).

o) UBE (*Unsolicited Bulk E-mail*) – Mensagens de *e-mails* não-solicitados em grande quantidade;

p) UCE (*Unsolicited Comercial E-mail*) – Mensagens de *e-mails* comerciais não solicitados.

2.3.2 História

A história do spam iniciou no dia 12 de abril de 1994, quando dois advogados Canter e Siegel enviaram uma mensagem não-solicitada para todos os

grupos de discussão da USENET fazendo propaganda de uma loteria de *green cards*. Essa mesma mensagem já tinha sido enviada no dia 5 de março de 1994, sendo esta data considerada como “aniversário do *spam*”. (TEIXEIRA, 2004).

A autora cita ainda que exista outra versão, datada do dia 3 de maio de 1978, quando um profissional de marketing da *Digital Equipment Corporation* (DEC) enviou uma mensagem com propaganda dos novos modelos do computador DEC-20. (TEIXEIRA, 2004).

Um vídeo de comédia do grupo Monty Phyton chamado de “Spam” (1970) foi inspiração para o termo utilizado para mensagens não-solicitadas, conforme RFC 2635 (Don’t Spew: A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam)) de junho de 1999. (THE INTERNET ENGINEERING TASK FORCE, 2003a).

Fora da internet, SPAM é um presunto condimentado (**SP**iced h**AM**) fabricado pela Hormel Foods que não aprovou de ver o seu produto associado ao *spam* da internet. Recomenda-se utilizar letras minúsculas para mensagens não-solicitadas e maiúsculas para o produto alimentício. (ANTISPAM.br, 2013a).

2.3.3 Classificação

Segundo ANTISPAM.br (2013d, e, f, g) o spam é classificado em:

a) correntes – são textos que descrevem uma história antiga, promessas de riquezas, uma simpatia ou desejam sorte. Para evitar a quebra da corrente, no corpo do texto é dito que a interrupção da corrente pode trazer azar, pobreza e outras tragédias, induzindo um processo contínuo de propagação. Exemplo: Corrente Ação entre Amigos;
b) boatos (*hoaxes*) – são mensagens que tem como conteúdo histórias alarmantes e falsas como: casos de crianças com doenças graves ou raras; o controle internacional da região Amazônica e o Pantanal;
c) lendas urbanas – são textos tristes, alegres, assustadores ou misteriosos, muito semelhante ao boatos. Diferem-se pelas justificativas para dar veracidade ao fato através de frases como: “Aconteceu com o primo do amigo do meu pai...” ou “O avô do marido da minha prima disse que foi mesmo verdade...”. Exemplo: Cobra em piscina de bolinhas;

d) propagandas – são mensagens com publicidade de produtos, serviços, sites e outros. Exemplos: Pílulas para perder peso dormindo ou para melhorar o desempenho sexual;
e) ameaças, brincadeiras e difamação – são textos com contendo ameaças, brincadeiras inconvenientes ou difamação de pessoas;
f) pornografia – são mensagens com conteúdo pornográfico;
g) códigos maliciosos – são *e-mails* que trazem em anexos códigos maliciosos como *backdoor* (invasão), *spyware* (monitorar as atividades do sistema), *keylogger* (capturar e armazenar teclas digitadas), *screenlogger* (capturar e armazenar telas apresentadas no monitor ou posições do mouse) e cavalo de tróia (programa para executar funções para o qual foi projetado);
h) Fraudes e golpes – são mensagens que induzem ao usuário em fornecer seus dados pessoais, contas e senhas bancárias e de cartões de crédito. Exemplos: Débitos ou pendências financeiras em bancos ou orçamentos, cotação de preços e lista de produtos.

2.3.4 Impactos

Os problemas causados pelo spam podem ser classificados em: os que afetam os usuários e os que afetam empresas ou provedores: (CENTRO..., 2012)

a) Usuários:

a) perda de mensagens importantes – devido ao grande volume de mensagens não-solicitadas, pode ocorrer de não ler ou apagar *e-mails* importantes ou ainda, de lê-las com atraso;
b) conteúdo impróprio ou ofensivo – existe uma grande chance de um usuário receber um *e-mail* com conteúdo impróprio ou ofensivo, devido que esses *spams* são enviados para endereços aleatórios de *e-mail*;
c) gasto necessário de tempo – um usuário necessita gastar um tempo para identificar, ler ou remover cada *spam* da caixa postal, gerando perda de tempo desnecessário e de produtividade;
d) não recebimento de *e-mails* – alguns serviços de *e-mail* limitam o

tamanho da caixa postal, correndo o risco de lotá-lo, impedindo de receber novas mensagens até que se consiga liberar espaço;

e) classificação errada de mensagens – utilizando-se de sistemas de filtragem com regras ineficientes de *antispam*, existe a possibilidade de mensagens legítimas serem apagadas, movidas para quarentena ou encaminhadas para outras pastas. Em alguns casos, classificadas como *spam*;

f) prejuízos financeiros causados por fraudes – o *spam* tem sido utilizado para difundir esquemas fraudulentos, ocasionando o furto de dados pessoais e financeiros; (ANTISPAM.br, 2013c).

g) aumento de custos – os provedores para amenizar os problemas, aumentam os recursos computacionais, transferindo os custos para as mensalidades dos usuários.

b) Empresas e Provedores:

a) impacto na banda – o alto volume de mensagens não-solicitas geram aumento no tráfego, sendo necessário a ampliação dos *links* para a internet;

b) má utilização dos servidores – consomem-se boa parte de recursos como tempo de processamento e espaço em disco no tratamento do *spam*;

c) inclusão em listas de bloqueio – empresas e provedores que enviam *spam* podem ter sua rede de endereçamento IP incluída em *blacklists*, prejudicando o envio de *e-mails*, resultando em perda de clientes;

d) investimento extra em recursos – aumento de investimento para aquisição de equipamentos e sistemas de filtragem e contratação de técnicos especializados na sua operação.

Conforme mencionado no capítulo 1, outro problema relevante é o consumo anual de energia elevado na faixa de 33 bilhões de quilowatts hora (kWh) com spam em 2008. (McAFEE, ICF, 2013)

Para Teixeira (2004), “o *spam* pode desacreditar o *e-mail* como ferramenta de comunicação à medida que coloca em xeque sua eficácia e credibilidade, contaminando as caixas de entrada com *e-mails* ilegítimos”. (TEIXEIRA, 2004)

2.3.5 Estatísticas no Brasil

As estatísticas apresentadas neste trabalho foram consultadas no CERT.br que é responsável por tratar incidentes de segurança que envolvam redes conectadas à internet brasileira. Outra atividade desse órgão é de manter estatísticas públicas dos incidentes tratados e das reclamações de *spam* recebidas. (CENTRO..., 2013a).

Segundo o CERT.br, as estatísticas geradas são obtidas das reclamações feitas ao SpamCop e ao Abusix.org e encaminhas ao CERT.br. As informações estão consolidadas de 2003 até 2012 e parcial até junho de 2013, conforme Figura 4 e Figura 5. (CENTRO..., 2013a).

Observam-se nas Figura 4 e Figura 5, que os anos de 2009 e 2010 ocorreram uma grande quantidade de *spams* reportados e para o ano 2011 houve uma queda acentuada. Provavelmente, reflexo do acordo de cooperação entre o CGI.br, Anatel , Ministério Público, órgão de defesa do consumidor, empresas de telefonia fixo e móvel e provedores de acesso e serviço de internet para o gerenciamento da porta 25.

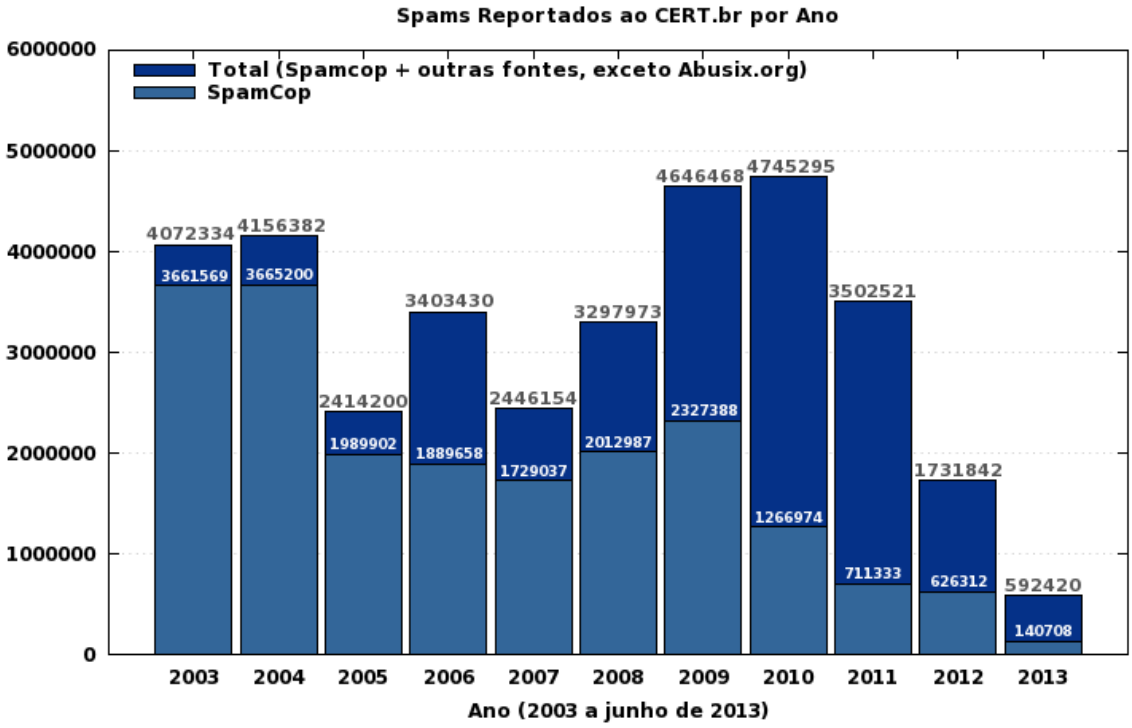


Figura 4 – Quantidade de spams reportados ao CERT.br de 2003 até junho de 2013, excluindo-se Abusix.org.
Fonte: http://www.cert.br/stats/spam/

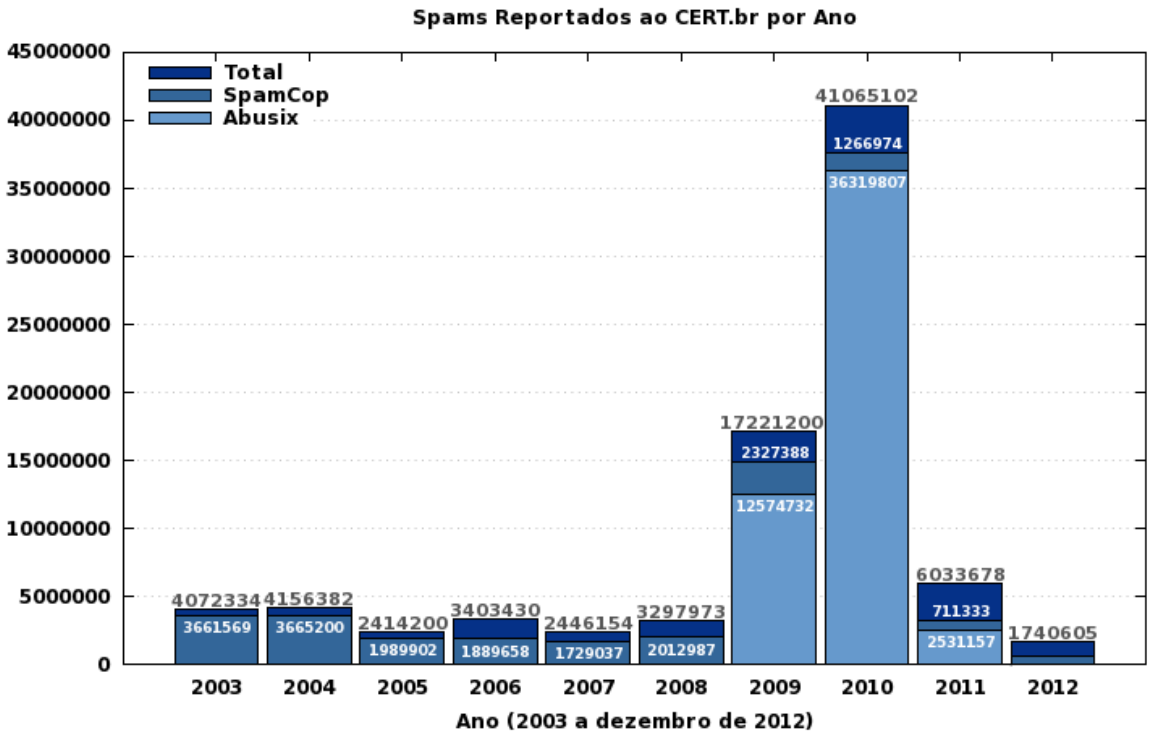


Figura 5 – Quantidade de spams reportados ao CERT.br de 2003 até dezembro de 2012.
Fonte: http://www.cert.br/stats/spam/

2.4 Listas negras *(blacklists)*

2.4.1 Funcionamento geral

As listas negras (*blacklists*) também são conhecidas como *Realtime Blackhole Lists* (RBLs) e são mantidas por organizações *anti-spam* que a atualizam regularmente. (TEIXEIRA, 2004).

As atualizações podem ocorrer de duas formas:

a) através de denúncias de servidores comprometidos com relay aberto. Após verificação, o IP é incluído na lista negra e os responsáveis avisados. (TEIXEIRA, 2004).

b) utilizando-se honeypots de baixa interatividade que são computadores configurados com emuladores de sistemas operacionais e de aplicativos e serviços, conforme Figura 6. Quando o spammer interage com o honeypots para envio de spam, ele é levado a acreditar que está conseguindo enviar os seus e-mails. O que acontece é que nenhum e-

mail é enviado, mas apenas coletado para estudos e inclusão nas listas negras. (CENTRO..., 2013b).

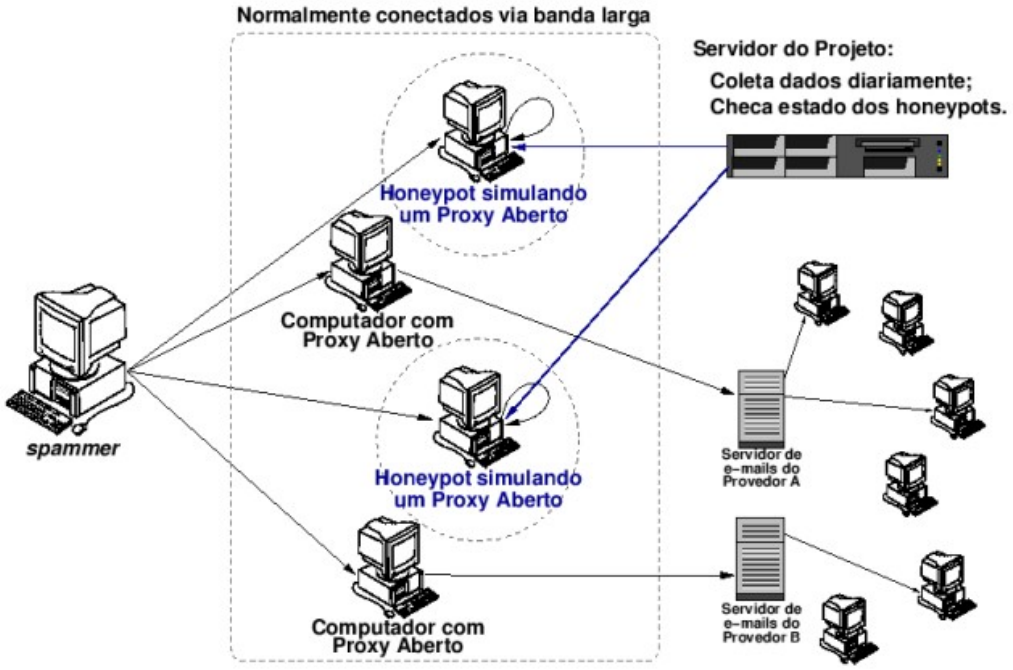


Figura 6 – Arquitetura de um *honeypots* de baixa interatividade.
Fonte: http://www.cert.br/docs/whitepapers/spampots/

A utilização das listas negras são implementadas facilmente pelos servidores de *e-mails* (MTAs) que consultam as mensagens vindas de endereços IPs contidos nestas listas e tomam a seguinte decisão:

a) descartar, notificando ou não a origem que a mensagem foi classificada como *spam*;
b) marcar as mensagens como [*spam*] e enviar assim mesmo.

Além das listas públicas, é possível criar *blacklists* próprias com endereços IP que violem alguma política pré-estabelecida. (ANTISPAM.br, 2013b).

Observou-se que não existe uma padronização entre as listas negras públicas na maneira que trabalham, isto é, algumas listam apenas o endereço IP que está praticando *spam*, outros tem critérios mais rígidos além dos IPs, listam blocos de endereçamento e até o ASN que é o caso da *blacklist* UCEPROTECT®-NETWORK.

2.4.2 Funcionamento específico da UCEPROTECT®-NETWORK

Será abordado o funcionamento da *blacklist* UCEPROTECT®-NETWORK porque a Copel Telecomunicações acabou optando pela sua utilização depois de testar várias outras *blacklists* devido a sua facilidade de consulta para verificar a eficácia no gerenciamento da porta 25 (SMTP). Cabe ressaltar que os serviços de e-mails da Copel são mantidos pela administração de redes da TI que é outra área dentro da empresa.

Segundo o site da empresa (http://www.uceprotect.net), a missão do projeto é acabar mundialmente com os abusos de *spam*.

Possui mais de 50 servidores distribuídos por vários países. E a manutenção e atualização das informações são de três formas:

a) sistemas de relatórios confiáveis utilizando-se de fontes como *spamtraps* (armadilhas) distribuídos;
b) pessoas anônimas ou que distribuem os *spamtraps* do projeto;
c) membros da UCEPROTECT-Orga que é um círculo exclusivo de técnico qualificados aceitos somente por convite que podem incluir ou remover manualmente IPs listados.

As consultas podem ser realizadas por IP ou ASN. Para a Copel Telecomunicações foi bastante interessante à consulta por ASN, já que os IPs estão classificados, não necessitando um tratamento de filtragem de IPs que pertencem ao ASN. Outras duas consultas interessantes são os TOP 10 e o *Pillory*, sendo que o primeiro mostra os 10 e o segundo apresenta todos os ASNs comprometidos.

Trabalha com três políticas de níveis:

a) Nível 1 (*Conservative*) – contém apenas endereços IPs únicos (/32). O IP permanece listado por 7 dias, caso não haja nenhuma recorrência. Enquanto houver recorrências o IP permanece listado até expirar o prazo de 7 dias da última recorrência. No exemplo da Figura 7, o IP com endereçamento final 68.2 foi listado uma única vez (1 *hits*) no dia 16/07/2013 às 21:19 e permanecerá até o dia 23/07/2013 às 23:00 Algumas vezes acontece de um IP ter várias recorrências (*hits*) e as datas mostradas são sempre da última ocorrência, como é o caso do IP com final 172.36 que teve 8 ocorrências, sendo a última no dia 20/07/2013 às 17:27 e data de expiração para 27/07/2013 às 19:00.

IP	Hits	Latest Impact +/- 1 Minute	Earliest Expiretime
[redacted].68.2	1	16.07.2013 21:19	23.07.2013 23:00
[redacted].172.36	8	20.07.2013 17:27	27.07.2013 19:00

Figura 7 – Exemplo de dois IPs listados no nível 1.
Fonte: http://www.uceprotect.net/en/rblcheck.php#

b) Nível 2 (*Strict*) – escalona para a alocação de blocos de endereçamentos IPs. Essa alocação é função da quantidade de IPs listados pela máscara do bloco, conforme critérios da Tabela 1 (são os valores mínimos para o bloco ser listado). Não foi observado escalonamento para máscaras menores que /24, isto é, /25 e /26.

Tabela 1 – Critério para escalonamento de blocos de endereçamento IPs.

Máscara	Quantidade de IPs
/26	1
/25	2
/24	**5**
/23	10
/22	15
/21	25
/20	40
/19	65
/18	105
/17	170
/16	275

Fonte: http://www.uceprotect.net/

Abaixo dos valores das Tabela 1 o *site* informa através de cores o *status* que o bloco de endereçamento IP se encontra, conforme

equação (2.1) e Tabela 2.

$$x = \frac{\text{nº IPs listados}}{\text{Limite máscara}} \tag{2.1}$$

Tabela 2 – Definição de status em função do critério (x)

Critério (x)	Status
x < 0,25	Not listed
0,25 ≤ x < 0,50	Attention
0,50 ≤ x < 0,75	Warning
0,75 ≤ x < 1,00	Alert
x ≥ 1,00	Listed

Fonte: http://www.uceprotect.net/

Na Figura 8 tem-se exemplos das mudanças de *status* de vários blocos de endereçamento IP. Exemplo: a rede com final 128.0/21 está com 16 IP listados e o limite para está mascara é 25, conforme Tabela 1 ou Figura 8. Da equação (2.1) obtêm-se:

$$x = \frac{\text{nº IPs listados}}{\text{Limite máscara}}$$
$$x = \frac{16}{25} = 0{,}64 \tag{2.2}$$

Pesquisando-se na Tabela 2, o valor de x=0,64 está entre 0,50 ≤ x < 0,75 tendo como resultado o *status* de *Warning* (cor laranja).

[redacted].84.0/22	NOT LISTED	0	15
[redacted].128.0/20	ALERT Extreme Listingrisk	31	40
---> [redacted].132.0/24	LISTED	7	5
---> [redacted].136.0/24	LISTED	5	5
[redacted].128.0/21	WARNING High Listingrisk	16	25
[redacted].136.0/21	WARNING High Listingrisk	15	25
[redacted].144.0/20	NOT LISTED	7	40
[redacted].144.0/21	NOT LISTED	4	25
[redacted].152.0/21	NOT LISTED	3	25
[redacted].160.0/20	ATTENTION Increased Listingrisk	18	40

Figura 8 - Exemplo de *status* de blocos de endereçamento IP.
Fonte: http://www.uceprotect.net/

c) Nível 3 (*Draconic*) – Neste nível é apresentada a reputação do ASN. Para definir o valor mínimo de IPs para listar o ASN depende de dois critérios:

a) Para até 50.000 IPs o valor mínimo é definido pela equação (2.3):

$$x = \frac{n^{o}\ \text{IPs listados nível 1}}{100} \qquad (2.3)$$

b) Para mais de 50.000 IPs o valor mínimo é definido pela equação (2.4):

$$x = \frac{n^{o}\ \text{total IPs do AS}}{0{,}2\%} \qquad (2.4)$$

Para outros valores abaixo do mínimo, os resultados apresentam uma graduação no *status* através de cores conforme Tabela 2.

Na Figura 9 observa-se que o ASN 14868 está com ótima reputação, pois possui apenas um 1 IP listado do total de 47.104 IPs. Como possui menos de 50.000 IPs para ter o ASN listado é necessário 100 IPs listados no nível 1 ou utilizar a equação (2.3).

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	NOT LISTED	47104	1 (0.002 %)	100	Not available

Figura 9 – Nível 3 – Mostra a reputação do ASN 14868.
Fonte: http://www.uceprotect.net/

3 ESTUDO E IMPLEMENTAÇÃO DO PROCESSO DE GERENCIAMENTO DA PORTA 25 (SMTP)

3.1 INTRODUÇÃO

Neste capítulo será abordado o estudo e o processo utilizado para implementar o gerenciamento da porta 25 através da aplicação de filtros e apresentar os resultados obtidos desde setembro de 2010.

3.1.1 Produtos de internet da Copel Telecomunicações

Basicamente a Copel Telecomunicações tem dois produtos de internet: IP Direto e a Banda Extra Larga (BEL). As características básicas dos produtos são descritas na Tabela 3.

Tabela 3 – Características básicas dos produtos de internet da Copel Telecomunicações

Produto	Público	Banda	Número de IPs
IP Direto	Pequenas, médias e grandes empresas; Serviços Públicos.	Simétrica com várias velocidades.	5 IP fixos (/29)
BEL Fibra Residencial e Empresarial	Residências; Pequenas, médias e grandes empresas; Serviços públicos.	Simétrica com velocidades de 20, 40, 60, 80 e 100Mbps.	1 IP dinâmico (/32)

Fonte: http://www.copeltelecom.com/

3.1.2 Cenário até agosto de 2010

O cenário até agosto de 2010 com problemas envolvendo IPs listados em RBLs eram grandes e refletiam no aumento das ordens de serviços (OS) abertas pelos clientes, provavelmente reflexo desse ano ter sido o campeão em volume de *spams* conforme estatística do CERT.br (item 2.3.5). O problema mais relatado era que não estavam conseguindo enviar *e-mails*. Verificou-se que o principal motivo era

porque IPs da sua própria sub-rede ou de sub-redes vizinhas estavam listados.

Após essa queixa, era solicitada a retirada do IP das listas negras, mas, isto podia demorar de algumas horas até alguns dias. Outro problema, era a cobrança realizada por algumas delas. Alguns clientes que não queriam esperar o prazo, solicitavam a troca da sub-rede, ocasionando retrabalho com a reconfiguração do circuito e a alteração da designação junto ao Registro de Domínios para a Internet no Brasil (Registro.br), ficando a Copel Telecomunicações com o “bloco sujo”.

Esse processo citado era ineficaz porque muitas vezes os IPs retornavam para as listas negras.

Iniciou-se um estudo para levantar a extensão de IPs listados. Cabe ressaltar que a Copel Telecomunicações não provê serviços de correio eletrônico, mas estava sofrendo dos problemas provocados pelos seus clientes que possuíam esse serviço.

Foram consultadas várias listas, mas encontraram-se dois problemas como:

a) permitir a pesquisa de um único IP por vez;
b) o fornecimento de arquivo com todos os IPs listados, necessitando filtrar para a retirada dos IPs pertencentes as redes da Copel Telecomunicações;

Optou-se pela utilização da lista UCEPROTECT®-NETWORK por sua facilidade de pesquisa por ASN, apresentar os IPs já filtrados (Figura 7), mostrar de forma gráfica através de cores a situação de cada sub-rede (Figura 10) e por não trazer muita variação em relação a outras listas públicas.

Figura 10 – Resultado da consulta feita no dia 16/09/2010, apresentando a situação de cada sub-rede e do ASN através de cores.
Fonte: http://www.uceprotect.net/

Da consulta do dia 16 de setembro de 2010 (Figura 10), podem-se exprimir as seguintes informações:

a) existem várias sub-redes em diversos níveis de situações (não listados até listados);
b) o ASN 14868 está com *status* de alerta;
c) tinha 98 IPs listados, representando 0,319% do total de 30.720 IPs do

ASN;

d) esses IPs foram listados mais de uma vez totalizando 1243 vezes (*hits*), e somente um deles entrou 59 vezes na *blacklist* (esse item aparece em outra consulta)*;*
e) nota-se 4 blocos /24 listados devido a 30 IPs, afetando diretamente 128 clientes (1 rede /24 pode ser dividida em 32 sub-redes /29);
f) seriam necessários mais 2 IPs listados para atingir o limite mínimo de nível 3 e o ASN seria listado.

3.1.3 Estratégia adotada

Após o levantamento da real situação do ASN em relação às *blacklists*, definiu-se que a estratégia adotada seria o gerenciamento da porta 25, em conformidade com a recomendação do CGI.br.

Os critérios adotados para o gerenciamento foram:

a) aplicação de filtro da porta 25 (SMTP) para os clientes que utilizam endereçamento IP da Copel Telecomunicações;
b) não seria aplicado filtro para os clientes que trocavam roteamento *Border Gateway Protocol* (BGP) com a Copel Telecomunicações e possuíam *Classless Inter-Domain Routing* (CIDR) próprio;
c) utilizar a *blacklist* UCEPROTECT®-NETWORK para verificar quais IPs estavam sendo listados e verificar a eficácia da aplicação do filtro;
d) aplicar o filtro de forma gradual, conforme os IPs eram listados e assim diminuir o impacto junto aos clientes;
e) comunicar o cliente através de e-mail, informando-o sobre a razão da aplicação do filtro, recomendar a utilização da porta 587 / Transmission Control Protocol (TCP) para submissão de e-mails entre cliente e servidor, solicitar o IP e o *Domain Name System* (DNS) reverso do(s) seu(s) servidor(es) de *e-mails* (se houvesse) e após um prazo de 7 dias úteis aplicar o referido filtro. A mudança da porta 25 para 587 deve-se que na porta 587 é devido a autenticação entre cliente-servidor.

Foi realizado um teste piloto no final de agosto e início de setembro de 2009 para avaliar os resultados. Infelizmente, não foram mantidos registros, mas o

resultado foi satisfatório.

3.1.4 Filtro da Porta 25

A estrutura do filtro é muito simples e consiste de 3 regras de *Access Control Lists* (ACL):

a) regra 1 – lista os IPs de origem (rede do cliente) que estão autorizados a enviar pacotes com destino para a 25/TCP;
b) regra 2 – lista os IPs de destino (SMTP *servers*) de alguns servidores externos que ainda não se adaptaram para receber *e-mails* pela porta 587/TCP;
c) regra 3 – bloqueia todo o tráfego com destino a porta 25/TCP que não tenha sido explicitamente liberado pelas duas regras anteriores.

Um exemplo de configuração de ACLs aplicado no roteador:

Regras ACLs
Regra 1 – IPs de origem – Servidor no cliente
acl number 2010 description ## PREFIXOS-ORIGEM-PERMITE - SPAM ## step 10 rule 10 permit source <*IP de origem 1*> 0 rule 20 permit source <*IP de origem 2*> 0
Regra 2 – IPs de destino – Servidor externos
acl number 3010 description ## PREFIXOS-DESTINO-PERMITE - SPAM ## rule 10 permit ip destination <*IP destino 1*> 0 rule 20 permit ip destination <*IP destino 2*> 0 rule 30 permit ip destination <*rede de destino 1*> 0.0.0.255 rule 40 permit ip destination <*rede de destino 2*> 0.0.0.63
Regra 3 – Bloqueio total
acl number 3020 description ## PORTA25-BLOQUEIO - SPAM ##

```
rule 10 deny tcp destination-port eq smtp
rule 1000 permit ip
```

Para os servidores de *e-mails* localizados no cliente, a liberação do filtro é feita pela regra 1. Se os servidores localizam-se fora da rede da Copel, aplica-se a regra 2 e caso o cliente não tenha servidor de e-mail a regra utilizada é a 3.

O filtro é compartilhado por todos os clientes e aplicado na interface do roteador que atende o circuito do cliente, conforme Figura 11.

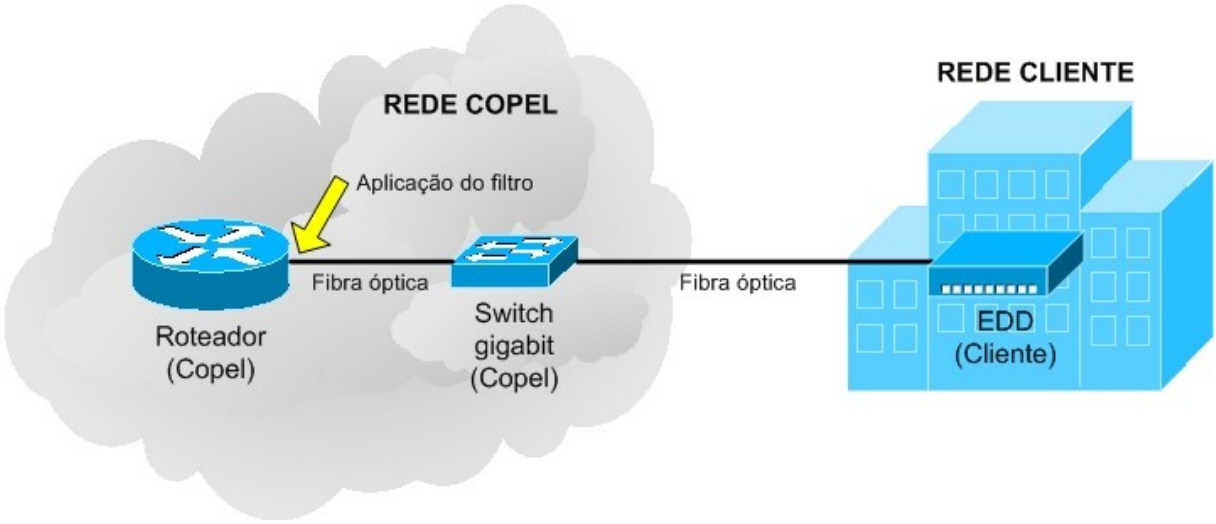


Figura 11 - Topologia de circuito utilizado para atender clientes.
Fonte: Própria

Um exemplo de configuração da aplicação do filtro na interface de cliente em um roteador:

Interface de cliente
interface GigabitEthernet1/0/0.1000 vlan-type dot1q 1000 description "Cliente – IP direto" bandwidth 10 ip address <*ip do gateway*> 255.255.255.248 **traffic-policy FILTRO-BLOCK-SPAM inbound** qos car cir 10000 cbs 1870000 pbs 0 green pass red discard inbound qos car cir 10000 cbs 1870000 pbs 0 green pass red discard outbound

statistic enable

Observa-se que a política “FILTRO-BLOCK-SPAM” é aplicada na interface do cliente no sentido de *inbound*, isto é, tráfego vindo do cliente para o roteador. Não há necessidade de aplicar o filtro no sentido *outbound* (roteador – cliente) porque se presume que o filtro deve-se sempre aplicar no sentido de origem para o destino das mensagens. A rede do cliente é submetida a essa política que consiste em chamar outra política de classificação (PERMITE-PREFIXO) e conforme o resultado é liberado ou não o serviço (LIBERA_BANDA).

Política do filtro – FILTRO-BLOCK-SPAM
traffic policy FILTRO-BLOCK-SPAM share-mode **classifier PERMITE-PREFIXOS behavior LIBERA_BANDA**

Na política de classificação que é verificado a aplicação das regras de ACLs.

Política de Classificação – PERMITE-PREFIXOS
traffic classifier PERMITE-PREFIXOS operator or if-match acl 2010 if-match acl 3010 if-match acl 3020

3.1.5 Procedimentos: clientes ativos e novos

O projeto piloto atendeu as expectativas e o gerenciamento da porta 25 passou fazer parte das atividades da área de suporte à clientes. Dessa experiência, resultou na elaboração de um procedimento para os clientes ativos, conforme Figura 12.

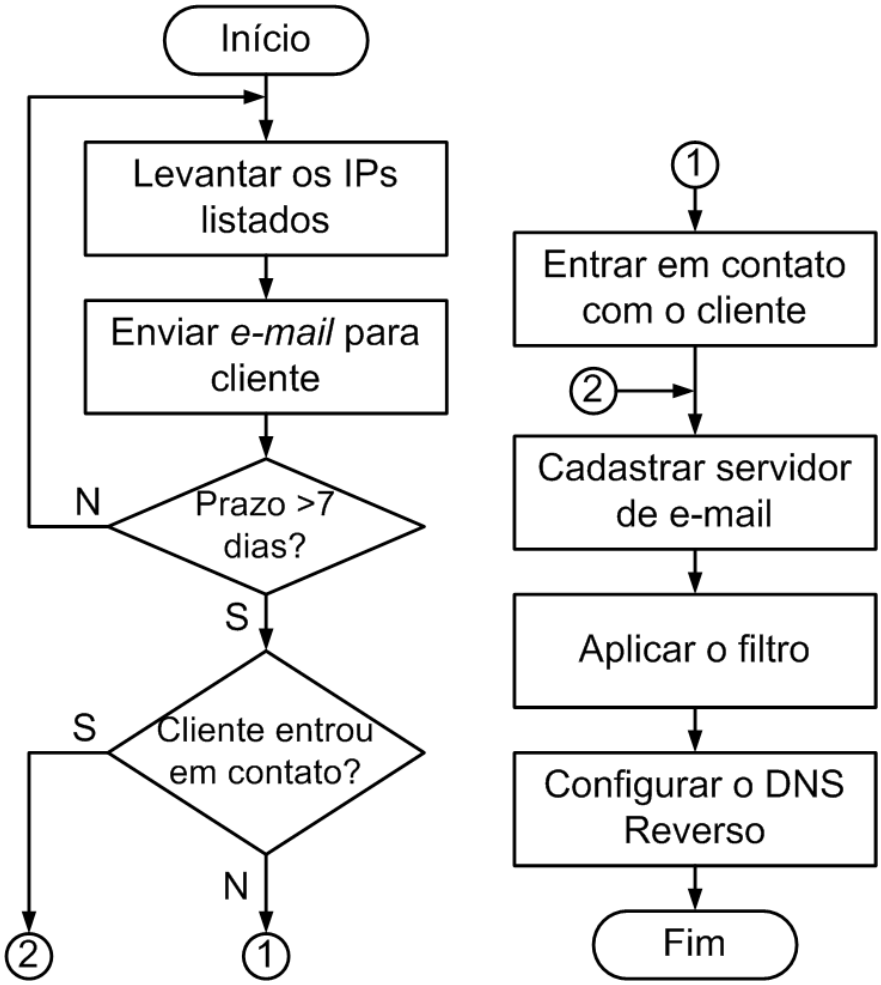


Figura 12 – Fluxograma para o gerenciamento da porta 25 de clientes ativos.
Fonte: Própria

Do fluxograma da Figura 12 tem-se:

a) levantar os IPs listados – diariamente é consultado a lista UCEPROTECT®-NETWORT para verificar os IPs listados;
b) enviar *e-mail* para o cliente – enviado *e-mail* para o cliente informando a razão do gerenciamento da porta 25; recomendar a utilização da porta 587/TCP para submissão das mensagens entre cliente-servidor; solicitar o(s) IP(s) e o(s) DNS reverso(s) do(s) servidor(es) de *e-mail* e informando que o filtro será aplicado em 7 dias úteis.
c) entrar em contato com o cliente – após o prazo de 7 dias úteis observou-se que muitos clientes não respondiam as solicitações de IPs e DNS reversos. É entrado em contato com o cliente por telefone para ver o motivo da falta de resposta. As respostas geralmente são que tinham esquecido;

d) cadastrar servidor de *e-mail* – os IPs dos servidores de *e-mails* são cadastrados no banco de dados com as informações técnicas do circuito do cliente;
e) aplicar o filtro – é aplicado o bloqueio da porta 25 na interface do roteador que atende o cliente. Se o cliente informou o(s) IP(s) do(s) servidor(es), então é/são liberado(s) nas ACLs;
f) configurar o DNS reverso – é configurado o DNS reverso quando informado. Observou-se que muitos IPs são listados por falta do DNS reverso.

Mas, esse processo não estava completo, porque todos os dias são configurados novos circuitos e era ineficaz esperar que o circuito fosse para a lista negra para depois ser aplicado o filtro. Definiu-se que os circuitos novos teriam o filtro aplicado na fase de configuração.

Após a configuração de um cliente novo, sempre é enviado um *e-mail* para o cliente contendo informações técnicas como: endereçamento IP, servidores de DNS e outras observações. Alterou-se esse *e-mail* padrão e foram incluídas as mesmas informações do item b do fluxograma para clientes ativos, com exceção que o filtro já estava aplicado.

3.1.6 Resultados obtidos

Com os processos definidos e sendo executados para clientes ativos e novos, iniciou-se a monitoração dos dados para verificar a eficácia no gerenciamento da porta 25.

Os dados começaram a ser coletados no dia 09 de setembro de 2010 e a meta definida era manter o controle dos IPs listados abaixo de 10 IPs.

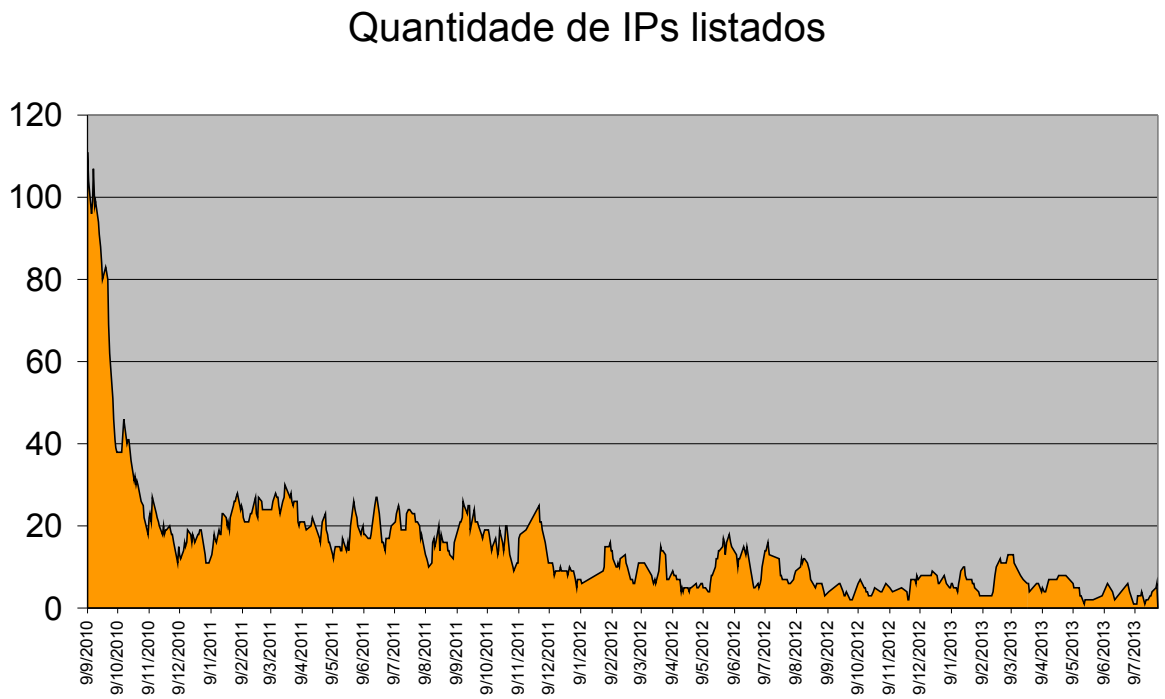


Figura 13 – Quantidade de IPs listados desde o dia 09 de setembro de 2010.
Fonte: Própria

Na Figura 13 tem-se a evolução dos IPs listados desde o dia 09 de setembro de 2010 até o dia 31 de julho de 2013. Observa-se que o gerenciamento da porta 25 foi eficaz porque diminui o número de IPs listados, mantendo-se abaixo ou muito próximo da meta estabelecida de 10 IPs. Do gráfico, obtêm-se algumas datas importantes:

Tabela 4 – Cronograma com alguns marcos importantes

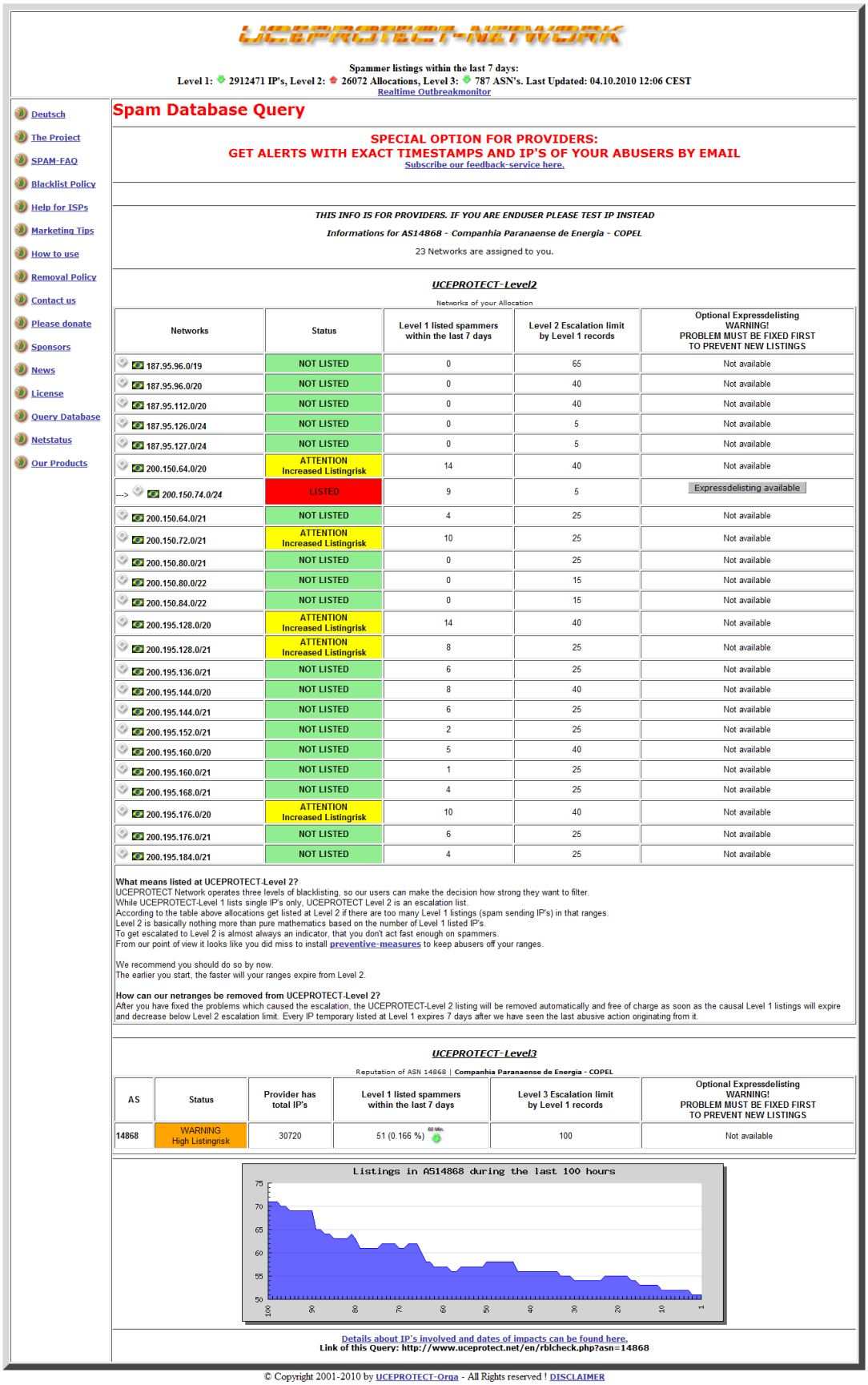
Data	Quantidade de IPs listados	Importância	Figura
09/09/2010	111	Início da monitoração. O ASN estava comprometido	-
16/09/2010	98	O ASN estava em estado de alerta	Figura 10
04/10/2010	51	Abaixo da metade do início da monitoração. Apenas um bloco /24 listado. O ASN estava em estado de advertência (*Warning*)	Figura 14
12/08/2011	10	Primeira vez que foi atingida a meta. Todos os blocos e o ASN não estavam listados.	-

Data	Quantidade de IPs listados	Importância	Figura
20/05/2013	1	Foi atingido o ponto mais baixo pela primeira vez. Todos os blocos e o ASN não estavam listados.	-

Fonte: Própria

Da consulta do dia 04 de outubro de 2010 (Figura 14), podem-se exprimir as seguintes informações:

a) Poucas sub-redes em situação de atenção;
b) o ASN 14868 está com *status* de advertência (*Warning*);
c) tinha 51 IPs listados, representando 0,166% do total de 30.720 IPs do ASN;
d) esses IPs foram listados mais de uma vez totalizando 399 vezes (*hits*), e somente um deles entrou 65 vezes na *blacklist* (esse item aparece em outra consulta e continua elevado)*;*
e) nota-se apenas 1 blocos /24 listados devido a 9 IPs, afetando diretamente 32 clientes;



UCEPROTECT-NETWORK

Spammer listings within the last 7 days:
Level 1: 2912471 IP's, Level 2: 26072 Allocations, Level 3: 787 ASN's. Last Updated: 04.10.2010 12:06 CEST
Realtime Outbreakmonitor

Deutsch
The Project
SPAM-FAQ
Blacklist Policy
Help for ISPs
Marketing Tips
How to use
Removal Policy
Contact us
Please donate
Sponsors
News
License
Query Database
Netstatus
Our Products

Spam Database Query

SPECIAL OPTION FOR PROVIDERS:
GET ALERTS WITH EXACT TIMESTAMPS AND IP'S OF YOUR ABUSERS BY EMAIL
Subscribe our feedback-service here.

THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

23 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
187.95.96.0/19	NOT LISTED	0	65	Not available
187.95.96.0/20	NOT LISTED	0	40	Not available
187.95.112.0/20	NOT LISTED	0	40	Not available
187.95.126.0/24	NOT LISTED	0	5	Not available
187.95.127.0/24	NOT LISTED	0	5	Not available
200.150.64.0/20	ATTENTION Increased Listingrisk	14	40	Not available
---> 200.150.74.0/24	LISTED	9	5	Expressdelisting available
200.150.64.0/21	NOT LISTED	4	25	Not available
200.150.72.0/21	ATTENTION Increased Listingrisk	10	25	Not available
200.150.80.0/21	NOT LISTED	0	25	Not available
200.150.80.0/22	NOT LISTED	0	15	Not available
200.150.84.0/22	NOT LISTED	0	15	Not available
200.195.128.0/20	ATTENTION Increased Listingrisk	14	40	Not available
200.195.128.0/21	ATTENTION Increased Listingrisk	8	25	Not available
200.195.136.0/21	NOT LISTED	6	25	Not available
200.195.144.0/20	NOT LISTED	8	40	Not available
200.195.144.0/21	NOT LISTED	6	25	Not available
200.195.152.0/21	NOT LISTED	2	25	Not available
200.195.160.0/20	NOT LISTED	5	40	Not available
200.195.160.0/21	NOT LISTED	1	25	Not available
200.195.168.0/21	NOT LISTED	4	25	Not available
200.195.176.0/20	ATTENTION Increased Listingrisk	10	40	Not available
200.195.176.0/21	NOT LISTED	6	25	Not available
200.195.184.0/21	NOT LISTED	4	25	Not available

What means listed at UCEPROTECT-Level 2?
UCEPROTECT Network operates three levels of blacklisting, so our users can make the decision how strong they want to filter.
While UCEPROTECT-Level 1 lists single IP's only, UCEPROTECT Level 2 is an escalation list.
According to the table above allocations get listed at Level 2 if there are too many Level 1 listings (spam sending IP's) in that ranges.
Level 2 is basically nothing more than pure mathematics based on the number of Level 1 listed IP's.
To get escalated to Level 2 is almost always an indicator, that you don't act fast enough on spammers.
From our point of view it looks like you did miss to install preventive-measures to keep abusers off your ranges.

We recommend you should do so by now.
The earlier you start, the faster will your ranges expire from Level 2.

How can our netranges be removed from UCEPROTECT-Level 2?
After you have fixed the problems which caused the escalation, the UCEPROTECT-Level 2 listing will be removed automatically and free of charge as soon as the causal Level 1 listings will expire and decrease below Level 2 escalation limit. Every IP temporary listed at Level 1 expires 7 days after we have seen the last abusive action originating from it.

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	WARNING High Listingrisk	30720	51 (0.166 %) 60 Min.	100	Not available

Details about IP's involved and dates of impacts can be found here.
Link of this Query: http://www.uceprotect.net/en/rblcheck.php?asn=14868

Figura 14 – Resultado da consulta feita no dia 04/10/2010
Fonte: http://www.uceprotect.net/

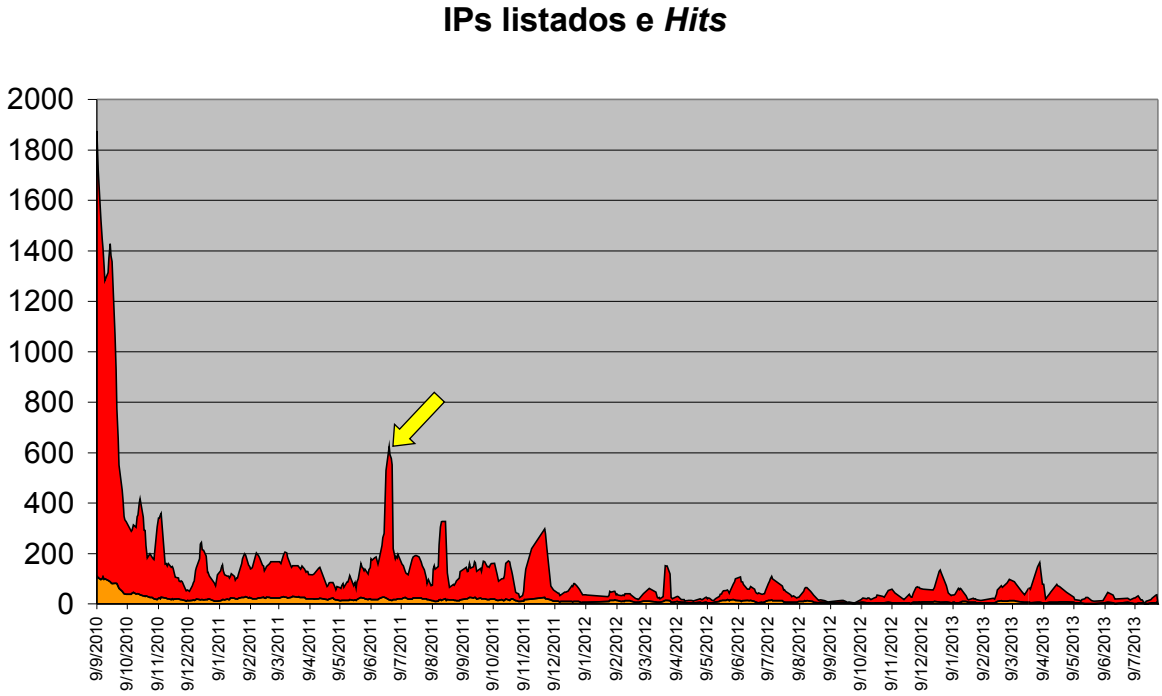


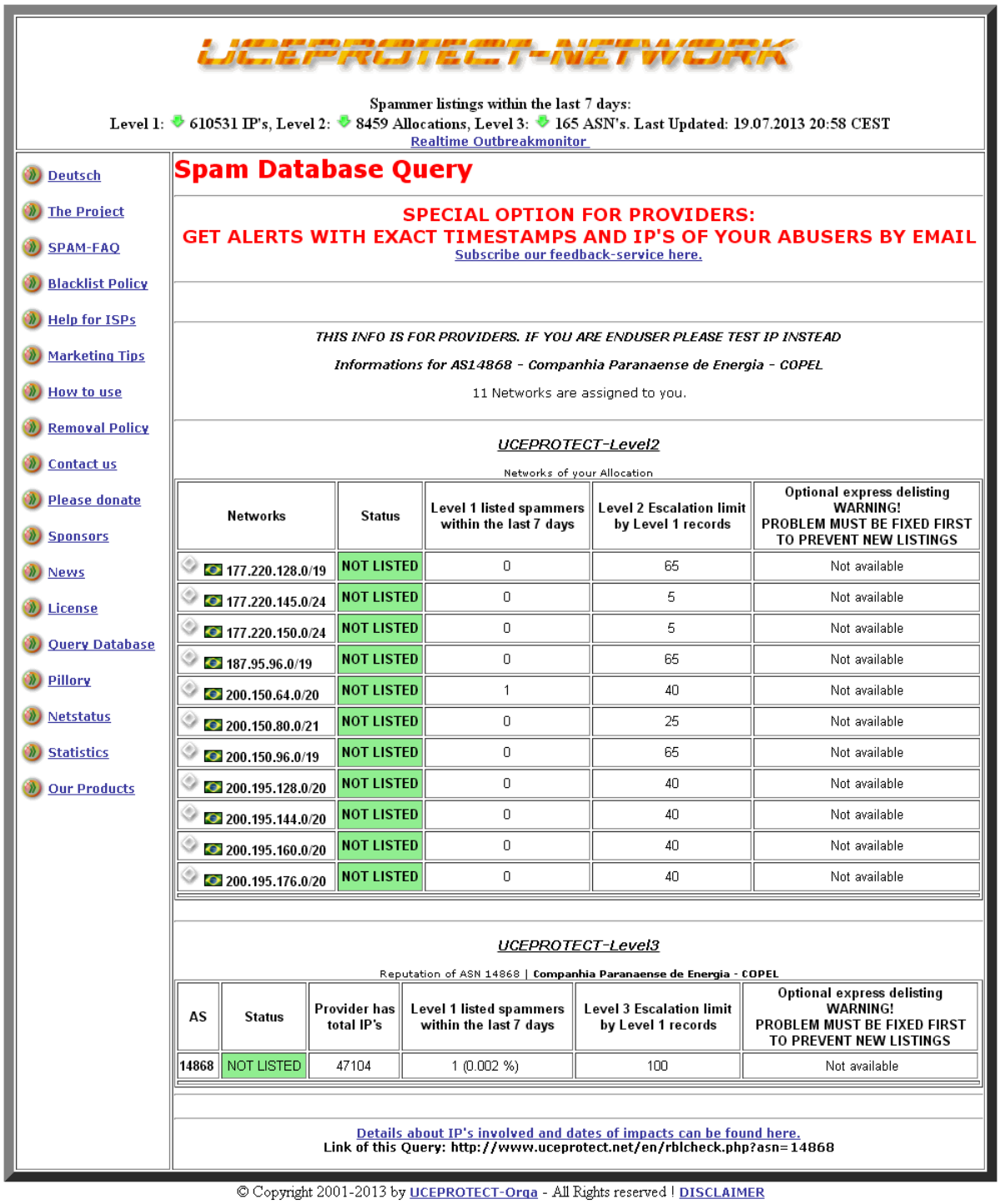
Figura 15 – Quantidade de IPs listados (laranja) e *hits* (recorrências em vermelho) desde o dia 09 de setembro de 2010.
Fonte: Própria

Na Figura 15 tem-se a evolução dos IPs listados e das recorrências (*hits*) desde o dia 09 de setembro de 2010 até o dia 31 de julho de 2013. Nota-se que a quantidade de ocorrências (*hits*) era muito grande em relação à quantidade de IPs. No dia 27 de junho de 2011 ocorreu um evento atípico (seta amarela), pois havia apenas 16 IPs listados, mas o número de ocorrências foi de 608. Analisou-se o fato e constatou-se que um único IP havia entrado 416 vezes na lista. Foi entrado em contato com o cliente para avisá-lo e que depois retornou com a informação que o servidor havia sido atacado.

3.1.7 Cenário até julho de 2013

Com o gerenciamento da porta 25, as OSs de clientes que não conseguem enviar e-mails acabaram. Atualmente, as OSs são abertas para configurar ou alterar endereços IP de servidores de *e-mail* ou DNS reverso.

Todos os blocos de endereçamento Ip e o ASN estão limpos conforme Figura 16.



UCEPROTECT-NETWORK

Spammer listings within the last 7 days:
Level 1: 610531 IP's, Level 2: 8459 Allocations, Level 3: 165 ASN's. Last Updated: 19.07.2013 20:58 CEST
Realtime Outbreakmonitor

Deutsch
The Project
SPAM-FAQ
Blacklist Policy
Help for ISPs
Marketing Tips
How to use
Removal Policy
Contact us
Please donate
Sponsors
News
License
Query Database
Pillory
Netstatus
Statistics
Our Products

Spam Database Query

SPECIAL OPTION FOR PROVIDERS:
GET ALERTS WITH EXACT TIMESTAMPS AND IP'S OF YOUR ABUSERS BY EMAIL
Subscribe our feedback-service here.

THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

11 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
177.220.128.0/19	NOT LISTED	0	65	Not available
177.220.145.0/24	NOT LISTED	0	5	Not available
177.220.150.0/24	NOT LISTED	0	5	Not available
187.95.96.0/19	NOT LISTED	0	65	Not available
200.150.64.0/20	NOT LISTED	1	40	Not available
200.150.80.0/21	NOT LISTED	0	25	Not available
200.150.96.0/19	NOT LISTED	0	65	Not available
200.195.128.0/20	NOT LISTED	0	40	Not available
200.195.144.0/20	NOT LISTED	0	40	Not available
200.195.160.0/20	NOT LISTED	0	40	Not available
200.195.176.0/20	NOT LISTED	0	40	Not available

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	NOT LISTED	47104	1 (0.002 %)	100	Not available

Details about IP's involved and dates of impacts can be found here.
Link of this Query: http://www.uceprotect.net/en/rblcheck.php?asn=14868

Figura 16 – Consulta feita no dia 19/07/2013
Fonte: http://www.uceprotect.net/

Mesmo com a aplicação do filtro para todos os blocos, alguns IPs continuam sendo listados porque são servidores de *e-mail* informados pelos clientes e seus IPs estão liberados em nosso filtro.

4 CONSIDERAÇÕES FINAIS

O filtro da porta 25 é simples. As dificuldades foram a definição dos procedimentos, a efetiva aplicação e principalmente manter o procedimento.

Nossos clientes conseguem enviar *e-mails* e não estão mais sendo punidos pelas *blacklists*.

Incentivamos aos nossos clientes a utilizar a porta 587 para submissão das mensagens entre cliente-servidor. Essa medida não elimina totalmente o problema de envio de *spams*, mas com a exigência de autenticação, o *spammer* deixa de ser “anônimo”.

Com a adoção do gerenciamento da porta 25, colabora-se para diminuição de *spams*, protegendo os blocos de endereçamento IP da Copel Telecomunicações, melhorando a sua reputação junto as listas negras, seus clientes e aos grupos de segurança e tratamento de incidentes do Brasil e do mundo.

Contribuí-se para melhorar a reputação do Brasil que caiu de segundo (2°) lugar em 2009 para vigésimo - sétimo (27°) lugar em 2013. (COMPOSITE..., 2013)

Outros operadores tem adotados medidas semelhantes

E, finalmente, o gerenciamento da porta 25 foi um sucesso.

REFERÊNCIAS BIBLIOGRÁFICAS

ANTISPAM.br. **História: origem e curiosidades**. Disponível em: <http://antispam.br/historia/>. Acesso em 26 mar. 2013a.

_____. **Listas de bloqueio**. Disponível em: <http://www.antispam.br/admin/listas-de-bloqueio/#2>. Acesso em 26 mar. 2013b.

_____. **Problemas causados pelo spam**. Disponível em: <http://antispam.br/problemas/>. Acesso em 26 mar. 2013c.

_____. **Tipos de spam**. Disponível em: <http://antispam.br/tipos/>. Acesso em 26 mar. 2013d.

_____. **Tipos de spam:** boatos. Disponível em: <http://antispam.br/tipos/boatos/>. Acesso em 26 mar. 2013e.

_____. **Tipos de spam:** códigos maliciosos. Disponível em: <http://antispam.br/tipos/malware/>. Acesso em 26 mar. 2013f.

_____. **Tipos de spam:** fraudes. Disponível em: <http://antispam.br/tipos/fraudes/>. Acesso em 26 mar. 2013g.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil:** do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. 239 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – COPPE, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, 2006. Disponível em: <http://tele.sj.ifsc.edu.br/~tisemp/RES/Internet-BR-Dissertacao.pdf>. Acesso em 08 mar. 2013.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.br. **Cartilha de Segurança para Internet:** versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 126 p.

_____. **Estatísticas de Notificações de *Spam* Reportadas ao CERT.br.** Disponível em: <http://www.cert.br/stats/spam/>. Acesso em: 18 jul 2013a.

_____. **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*.** Disponível em: <http://www.cert.br/docs/whitepapers/spampots/>. Acesso em: 18 jul 2013b.

COMER, Douglas E. **Redes de Computadores e a Internet:** abrange transmissão de dados, ligações inter-redes, web e aplicações. 4ª edição. Porto Alegre: Editora Bookman, 2007. 640 p.

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. **Resolução CGI.br/RES/2009/002/P – Recomendação para a adoção de Gerência de Porta 25 em Redes de Caráter Residencial**. São Paulo, SP, 24 abr. 2009. Disponível em: <http://www.cgi.br/regulamentacao/pdf/resolucao-2009-001.pdf>. Acesso em 08 mar. 2013.

COMPOSITE BLOCKING LIST - CBL. **CBL breakdown by Country, Highest by count**. Disponível em: <http://cbl.abuseat.org/country.html>. Acesso em 25 jul. 2013.

IDGNOW!. **E-mail comemora aniversário de trinta anos**. São Paulo, 10 maio 2012. Disponível em: <http://idgnow.uol.com.br/internet/2012/05/10/e-mail-comemora-aniversario-de-trinta-anos/>. Acesso em 08 mar. 2013a.

_____. **Brasil deixa lista de países que mais emitem spam no mundo, diz CGI.br**. São Paulo, 19 mar. 2013. Disponível em: <http://idgnow.uol.com.br/internet/2013/03/19/brasil-deixa-lista-de-paises-que-mais-emitem-spam-no-mundo-diz-cgi.br/>. Acesso em 19 mar. 2013b.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet:** uma nova abordagem. São Paulo: Editora Addison Wesley, 2003. 171 p.

McAFFE, ICF International. **The Carbon Footprint of Email Spam Report**. Disponível em: < http://www.mcafee.com/us/resources/reports/rp-carbonfootprint2009.pdf>. Acesso em 25 mar. 2013.

TEIXEIRA, Renata Cicilini. **Combatendo o spam:** aprenda como evitar e bloquear e-mails não-solicitados. São Paulo: Novatec Editora, 2004. 171 p.

THE INTERNET ENGINEERING TASK FORCE - IETF. **RFC 2635 – DON'T SPEW:** A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam). 1999. Disponível em: <http://www.rfc-editor.org/rfc/rfc2635.txt>. Acesso em 05 jul. 2013a.

_____. **RFC 5321 – Simple Mail Transfer Protocol.** 2008. Disponível em: <http://www.rfc-editor.org/rfc/rfc5321.txt>. Acesso em 05 jul. 2013b.