

Adoção de Gerência de Porta 25 no Mundo e Situação das Discussões no Brasil

Cristine Hoepers

cristine@cert.br

Klaus Steding-Jessen

jessen@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Núcleo de Informação e Coordenação do Ponto br

Comitê Gestor da Internet no Brasil

Agenda

Motivação

Gerência de Porta 25

- Benefícios

- Quem adota

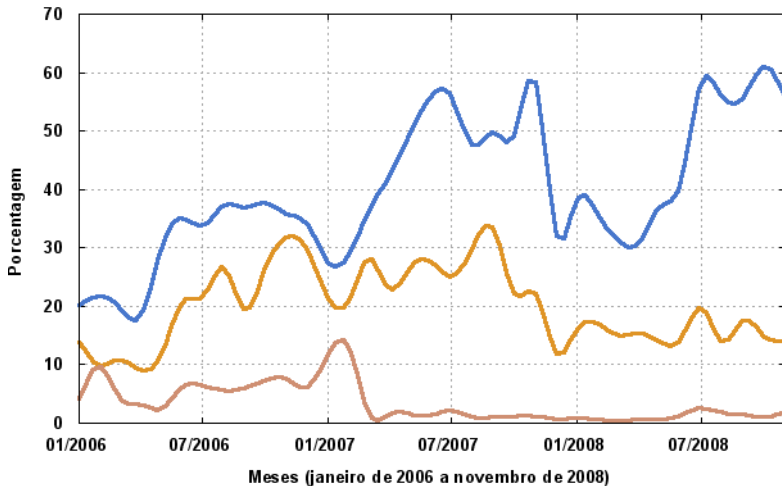
- Possíveis desafios do processo de implantação

- Evolução das discussões no Brasil

Referências

<http://www.cert.br/stats/spam/porcentagens/>

Porcentagem de Spams Reportados ao CERT.br
Categorias mais Comuns sobre o Total



Proxy Aberto

Envio Direto de Spam

Spamvertized Website

Brasil na CBL (1/2)

O Brasil é o país com maior número de IPs listados na CBL:

- 619.160 IPs listados (11.75%)
- Outros países com mais de 5%: TR (8.18%), RU (7.94%), CN (7.52%) e IN (7.08%)

“The CBL takes its source data from very large spamtraps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate etc) which have been abused to send spam, worms/viruses that do their own direct mail transmission (...)”

<http://cbl.abuseat.org/> – dados de 17/12/2008

Brasil na CBL (2/2)

Domínio (reverso)	Posição no Ranking	Número de IPs Listados	Porcentagem do Total
telebahia.net.br (Oi)	3	185.164	3.51
telesp.com.br	5	144.451	2.74
brasiltelecom.net.br	7	126.788	2.41
telet.com.br (Claro)	30	32.801	0.62
netservicos.com.br	35	28.619	0.54
gvt.net.br	49	18.926	0.36
ig.com.br	55	16.624	0.32
ctbctelecom.net.br	64	14.615	0.28
timbrasil.com.br	66	14.108	0.27
embratel.net.br	91	10.452	0.20
canbrasnet.com.br	128	6.654	0.13

Total de IPs na CBL: 5.270.878 – dados de 17/12/2008

Resultados do Projeto SpamPots

Métricas sobre o Abuso de Redes de Banda Larga para o Envio de *Spam*

Período de coleta	10/06/2006 a 18/09/2007
Dias coletados	466
Total de <i>emails</i>	524.585.779
<i>Emails</i> /dia	1,2 milhões
Destinatários	4.805.521.964
Destinatários/ <i>spam</i>	9,16
IPs únicos	216.888
ASNs únicos	3.006
<i>Country Codes</i>	165

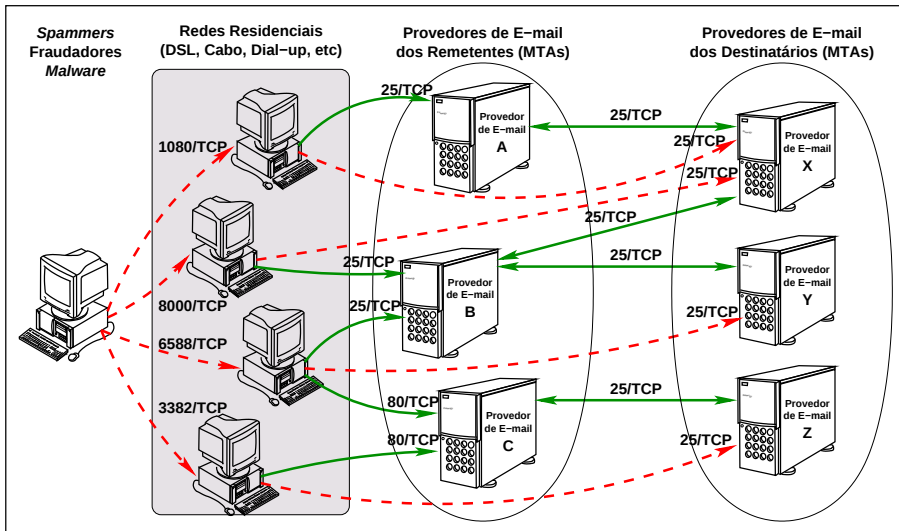
Principais Resultados:

- 99.84% das conexões eram originadas do exterior
- os *spammers* consumiam toda a banda de *upload* disponível;
- mais de 90% dos *spams* eram destinados a redes de outros países.

- Projeto mantido pelo CGI.br/NIC.br, como parte da CT-Spam
- 10 sensores (*honeypots* de baixa interatividade)
 - 5 operadoras diferentes de cabo e DSL
 - em conexões residenciais e comerciais

<http://www.cert.br/docs/whitepapers/spampots/>

Abuso – Cenário Atual



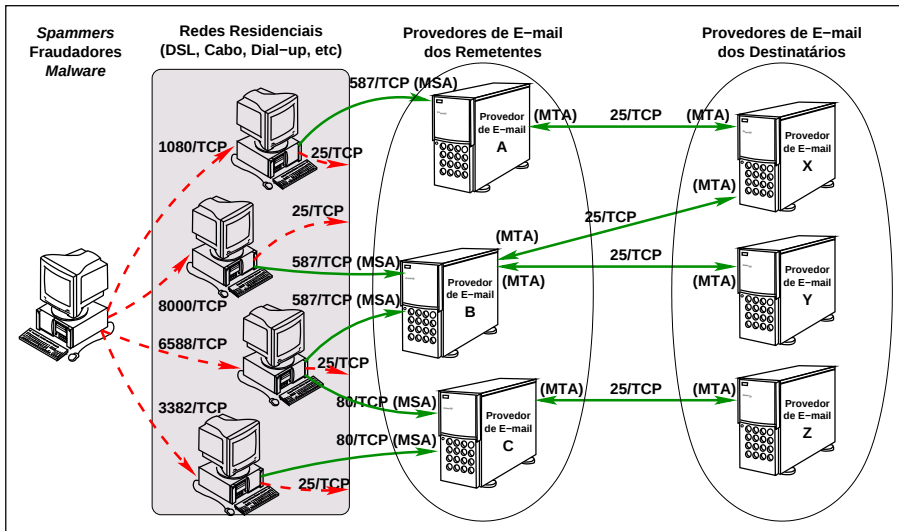
Gerência de Porta 25

Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

Implementação depende da aplicação de medidas por provedores e operadoras:

- Provedores de serviços de correio eletrônico:
 - Implementar o padrão de *Message Submission*, tipicamente na porta 587/TCP (RFC 4409), e implementar SMTP autenticado
- Operadoras de banda larga/*dial up* de perfil residencial (usuário final):
 - Impedir envio direto de mensagens eletrônicas (através da filtragem da saída de tráfego com destino à porta 25/TCP)

Gerência de Porta 25 e Seu Impacto



Benefícios

- Saída dos blocos das operadoras de listas de bloqueio
- Diminuição de reclamações de usuários
- 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*
- Diminuição do consumo de banda internacional por *spammers*
- Diminuição de custos operacionais
 - spam foi o mais apontado como responsável pela demanda de recursos operacionais no “*2008 Worldwide Infrastructure Security Report*”

<http://www.arbornetworks.com/report>

Quem Adota Gerência de Porta 25 (1/2)

Segundo a diretoria do MAAWG, todos os seus membros, que incluem: AT&T, Comcast, Earthlink, France Telecom, Verizon, Sprint, Time Warner Cable, Telefonica SA (EUA) e Bell Canada

Referências *on-line* sobre quem adota nos EUA:

- *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>

Quem Adota Gerência de Porta 25 (2/2)

- Sercomtel, no Brasil (Londrina/PR)
 - <ftp://ftp.registro.br/pub/gter/gter23/videos/mp4/gts-06-mail-submission.mp4>
- Europa
 - Segundo a ENISA, 50% dos ISPs Europeus consultados
http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf
 - S.I.A.S. (Swiss ISPs Against Spam): Bluewin, cablecom e green.ch
<http://www.stopspam.ch/engl/infos.htm>
- Japão
 - Recomendação do JEAG (Japan Email Anti-Abuse Group)
<http://jeag.jp/>

Possíveis Desafios do Processo de Implantação

- Carga no suporte dos provedores: precisam contactar o usuário final para alterar configurações
- Necessidade de diferenciar, nas operadoras, conexões residenciais de conexões comerciais
- Questões contratuais com clientes antigos
- Lidar com exceções
 - *softwares* desatualizados/antigos, sem suporte para *Message Submission*

Evolução das Discussões no Brasil (1/2)

21/06/2005: seminário com operadoras e provedores para discutir o documento “Tecnologias e políticas para Combate ao *Spam*”.

15/12/2005: discussão do documento na 5ª reunião ordinária do CBC-1 da Anatel.

12/07/2007 e 13/09/2007: reuniões entre operadoras, CERT.br e setor financeiro sobre o abuso das redes de banda larga para atividades maliciosas; como resultado destas discussões foi consenso que gerência de porta 25 deveria ser o primeiro tema a ser tratado, evidenciando a importância de envolver os provedores nas discussões.

Evolução das Discussões no Brasil (2/2)

08/11/2007: reunião entre operadoras, CERT.br, setor financeiro e provedores, sobre gerência de porta 25.

22/02/2008: discussão sobre gerência de porta 25 na 13ª reunião ordinária do CBC-1 da Anatel; nesta reunião o representante da Anatel solicitou às operadoras o estudo da viabilidade técnica de implantação e prazo necessário.

Referências

- Documentos e Palestras do CERT.br no Escopo do seu Trabalho na CT-Spam

<http://www.cert.br/docs/ct-spam/>

- Resultados Preliminares do Projeto SpamPots

<http://www.cert.br/docs/whitepapers/spampots/>

- Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction

<http://www.maawg.org/port25/>

- RFC 4409: Message Submission for Mail

<http://www.ietf.org/rfc/rfc4409.txt>

- RFC 5068: Email Submission Operations: Access and Accountability Requirements

<http://www.ietf.org/rfc/rfc5068.txt>